24 de agosto de 2020
Español
Original: inglés

Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020

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, 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 se celebró del 17 al 21 de enero de 2011 en Viena. En esa reunión, el Grupo de Expertos examinó y aprobó un conjunto de temas y una metodología para la realización del estudio (E/CN.15/2011/19, anexos I y II).

3. La segunda reunión del Grupo de Expertos se celebró en Viena del 25 al 28 de febrero de 2013. En esa reunión, el Grupo de Expertos tomó nota del proyecto de estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, que había preparado la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) con la orientación del Grupo de Expertos, de conformidad con el mandato contenido en la resolución 65/230 de la Asamblea General y el conjunto de temas y la metodología para la realización del estudio que se aprobaron en la primera reunión del Grupo de Expertos.

4. En la Declaración de Doha sobre la Integración de la Prevención del Delito y la Justicia Penal en el Marco Más Amplio del Programa de las Naciones Unidas para Abordar los Problemas Sociales y Económicos y Promover el Estado de Derecho a Nivel Nacional e Internacional y la Participación Pública, aprobada por el 13er Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y refrendada por la Asamblea General en su resolución 70/174, los Estados Miembros tomaron conocimiento de las actividades del Grupo de Expertos e invitaron a la Comisión de Prevención del Delito y Justicia Penal a que estudiara la posibilidad de recomendar que el Grupo de Expertos, basándose en su propia labor, siguiera intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales

respuestas y proponer nuevas respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional.

5. La tercera reunión del Grupo de Expertos se celebró en Viena del 10 al 13 de abril de 2017. En esa reunión, el Grupo de Expertos examinó, entre otras cosas, la posibilidad de aprobar los resúmenes del Relator sobre las deliberaciones de las reuniones primera y segunda del Grupo de Expertos, el proyecto de estudio exhaustivo del problema del delito cibernético y las observaciones recibidas al respecto, y el modo de avanzar con respecto al proyecto de estudio. También intercambió información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional.

6. En su resolución 26/4, aprobada en su 26º período de sesiones, celebrado en mayo de 2017, la Comisión de Prevención del Delito y Justicia Penal solicitó al Grupo de Expertos que prosiguiera su labor y, para ello, celebrara reuniones periódicas y funcionara como plataforma para impulsar el debate sobre cuestiones sustantivas relacionadas con el delito cibernético, siguiendo la evolución de las tendencias al respecto y en consonancia con la Declaración de Salvador y la Declaración de Doha. También en esa resolución, la Comisión solicitó al Grupo de Expertos que siguiera intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las respuestas actuales y proponer nuevas respuestas jurídicas o de otra índole a nivel nacional e internacional frente al delito cibernético.

7. La cuarta reunión del Grupo de Expertos se celebró en Viena del 3 al 5 de abril de 2018. En esa reunión, la labor del Grupo de Expertos se centró en la legislación y los marcos y en la tipificación en relación con el delito cibernético. Se examinaron las novedades legislativas y de políticas para hacer frente al delito cibernético a nivel nacional e internacional. El Grupo de Expertos estudió asimismo cómo se tipificaba la ciberdelincuencia a nivel nacional. También en esa reunión, el Grupo de Expertos aprobó el plan de trabajo del Grupo de Expertos propuesto por la Presidencia para el período 2018-2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. La quinta reunión del Grupo de Expertos se celebró en Viena del 27 al 29 de marzo de 2019. En esa reunión, el Grupo de Expertos se centró en la aplicación de la ley y las investigaciones, así como en las pruebas electrónicas y la justicia penal en relación con el delito cibernético. También en esa reunión el Grupo de Expertos examinó, entre otras cosas, las iniciativas que se habían puesto en marcha a nivel nacional con resultados satisfactorios para aplicar medidas jurídicas y de procedimiento destinadas a combatir el delito cibernético y medidas para aplicar nuevos instrumentos de investigación para obtener pruebas electrónicas y determinar su autenticidad a efectos probatorios en actuaciones penales. Asimismo, las deliberaciones se centraron en la manera de lograr un equilibrio entre la necesidad de articular respuestas eficaces a la ciberdelincuencia desde el punto de vista de los organismos encargados de hacer cumplir la ley y la protección de los derechos humanos fundamentales, en especial el derecho a la privacidad. El Grupo de Expertos concedió prioridad a la necesidad de una creación de capacidad sostenible para mejorar la capacidad nacional y permitir el intercambio de buenas prácticas y experiencias de investigación.

9. En su resolución 74/173, la Asamblea General reconoció la importancia de la labor del Grupo de Expertos para seguir intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a estudiar diferentes opciones para fortalecer las actuales respuestas jurídicas o de otra índole frente a la ciberdelincuencia a nivel nacional e internacional y proponer otras nuevas; observó con aprecio que el Grupo de Expertos formularía, de conformidad con su plan de trabajo para el período 2018-2021, posibles conclusiones y recomendaciones que presentaría a la Comisión de Prevención del Delito y Justicia Penal; reconoció que el Grupo de Expertos era un foro importante para el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional; solicitó a la UNODC que continuara recopilando información periódicamente sobre las novedades, los progresos y las mejores prácticas que se hubieran observado y siguiera comunicando periódicamente esa información al Grupo de Expertos y a la Comisión;

e invitó al Grupo de Expertos a que impartiera asesoramiento, basándose en su labor, a la UNODC, entre otras cosas con respecto al Programa Mundial contra el Delito Cibernético, a fin de ayudar a determinar cuáles eran las necesidades más prioritarias en materia de creación de capacidad y las medidas más eficaces para atenderlas, sin perjuicio de otras cuestiones previstas en el mandato del Grupo de Expertos ni de la condición de la Comisión en cuanto que órgano rector del programa contra el delito de la Oficina.

10. La Mesa ampliada del Grupo de Expertos aprobó las fechas originales del 6 al 8 de abril de 2020 para la sexta reunión del Grupo de Expertos mediante el procedimiento de acuerdo tácito el 11 de noviembre de 2019. El programa provisional de la sexta reunión fue acordado por la Mesa ampliada también mediante el procedimiento de acuerdo tácito el 18 de diciembre de 2019. El 12 de marzo de 2020, se informó a la Mesa ampliada de que se aplazaría la reunión debido a las restricciones relacionadas con la enfermedad por coronavirus (COVID-19). Mediante el procedimiento de acuerdo tácito, el 15 de abril de 2020 la Mesa ampliada aprobó nuevas fechas, del 27 al 29 de julio de 2020, para la celebración de la sexta reunión del Grupo de Expertos. La celebración de la sexta reunión en un formato híbrido/con presencia de la Presidencia fue aprobada mediante el procedimiento de acuerdo tácito el 22 de junio de 2020.

II. Lista de recomendaciones y conclusiones preliminares recopiladas por el Relator

11. De conformidad con el plan de trabajo del Grupo de Expertos para el período 2019-2021, el Relator, con la asistencia necesaria de la Secretaría y con arreglo a los debates y deliberaciones celebrados durante la reunión, preparó una lista de conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros, que son precisas y se centran en el fortalecimiento de las respuestas prácticas a la ciberdelincuencia. Conforme al plan de trabajo, la lista se ha incluido en el informe de la sexta reunión, en forma de recopilación de las sugerencias formuladas por los Estados Miembros para su posterior examen en la reunión que se celebre a más tardar en 2021 para hacer una evaluación.

12. Como se establece en el plan de trabajo, en la reunión que se celebrará para hacer una evaluación el Grupo de Expertos examinará la recopilación de conclusiones y recomendaciones preliminares y las compilará en una lista de conclusiones y recomendaciones aprobadas que se presentará a la Comisión de Prevención del Delito y Justicia Penal. Antes de la reunión de evaluación, las conclusiones y recomendaciones preliminares propuestas por los Estados Miembros se distribuirán a todos los Estados Miembros, observadores y otras partes interesadas para que formulen observaciones, y esas observaciones se publicarán en línea con anterioridad a dicha reunión para que las examinen las delegaciones.

A. Cooperación internacional

13. En consonancia con el plan de trabajo del Grupo de Expertos, el presente párrafo contiene una recopilación, preparada por el Relator, de las sugerencias formuladas por los Estados Miembros en la reunión relativas al tema 2 del programa, titulado “Cooperación internacional”. Las recomendaciones y conclusiones preliminares que figuran a continuación fueron presentadas por los Estados Miembros, y su inclusión en el presente documento no supone que el Grupo de Expertos las haya hecho suyas; tampoco están presentadas en orden de importancia:

a) En cuanto al alcance de la definición de “delito cibernético” a efectos de cooperación internacional, los países deberían tipificar como delito los actos de ciberdelincuencia en grado suficiente, de modo que quedaran comprendidos no solo los delitos basados en la cibernética, sino también otros delitos que con frecuencia se cometen utilizando Internet y medios electrónicos (delitos facilitados por la

cibernética), como el fraude cibernético, el robo cibernético, la extorsión, el blanqueo de dinero, el tráfico de drogas y armas, la pornografía infantil[1] y actividades terroristas.

b) En relación con los mecanismos de cooperación internacional, se alentó a los Estados a que, a falta de un tratado bilateral de asistencia judicial recíproca, utilizaran o se adhirieran a los tratados multilaterales existentes que proporcionan una base jurídica para la prestación de asistencia judicial recíproca, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia del Consejo de Europa. En ausencia de un tratado, los Estados podrían solicitar cooperación a otro Estado sobre la base del principio de reciprocidad; el Convenio sobre la Ciberdelincuencia del Consejo de Europa también debería usarse como referencia en la creación de capacidad y la asistencia técnica en todo el mundo, y se señaló la atención sobre las negociaciones en curso sobre el segundo protocolo adicional de ese instrumento para reforzar aún más la cooperación transfronteriza. Se reiteró la opinión de que el Convenio sobre la Ciberdelincuencia del Consejo de Europa tenía un ámbito de aplicación limitado por su condición de instrumento regional y su

[1] La expresión “pornografía infantil” está cimentada firmemente en instrumentos jurídicos internacionales aprobados en el siglo XXI. En el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía se define la expresión “pornografía infantil” en su artículo 2 como “toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales”. Además, con arreglo al artículo 3, párrafo c) de ese Protocolo Facultativo, los Estados deben tipificar como delito los siguientes elementos constitutivos del delito de pornografía infantil: “La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil, en el sentido en que se define en el artículo 2”. El Convenio sobre la Ciberdelincuencia del Consejo de Europa, en su artículo 9, párrafo 2, hace referencia a la expresión “pornografía infantil”, que se define como “material pornográfico que contenga la representación visual de: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito; y c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito”. El artículo 20, párrafo 2, del Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual contiene la expresión “pornografía infantil”, que se define como “todo material que represente de forma visual a un niño manteniendo una conducta sexualmente explícita, real o simulada, o toda representación de los órganos sexuales de un niño con fines principalmente sexuales”. Con arreglo al artículo 20, párrafo 1, de esa Convención, las partes deben tipificar como delito “la producción de pornografía infantil, la oferta o puesta a disposición de pornografía infantil, la distribución o transmisión de pornografía infantil, la adquisición para sí o para otro de pornografía infantil, la posesión de pornografía infantil, y el acceso a pornografía infantil, con conocimiento de causa y por medio de las tecnologías de la información y la comunicación”.
Lo expuesto anteriormente ha contribuido a que se utilice la expresión “pornografía infantil” en legislación nacional. Así pues, la expresión sigue siendo importante para la definición de un delito en muchos países. No obstante, existe una tendencia creciente, tanto entre los órganos encargados de hacer cumplir la ley como entre los organismos de protección de la infancia, a cuestionar la idoneidad de la expresión y a sugerir una terminología alternativa (véase Grupo de Trabajo Interinstitucional sobre Explotación Sexual de Niñas, Niños y Adolescentes, *Orientaciones Terminológicas para la Protección de Niñas, Niños y Adolescentes contra la Explotación y el Abuso Sexuales,* Bangkok, ECPAT International, 2016, págs. 38 a 40).
Por ello, aunque la expresión “pornografía infantil” sigue utilizándose ampliamente, se ha venido utilizando cada vez más la expresión “material que muestra abusos sexuales de niños” para describir representaciones sexualmente explícitas de niños, ya que se considera que esa expresión refleja con mayor precisión la naturaleza grave del contenido y cuestiona cualquier noción de que esos actos pueden llevarse a cabo con el consentimiento del niño. Por ejemplo, en el Proyecto relativo al Material que Muestra Abusos a Menores en Internet, de la iniciativa Planificación Estratégica Operacional General de la Policía, se defiende la noción de que una imagen sexual de un niño es un abuso o una explotación y nunca debe describirse como pornografía. “Pornografía” es un término que se utiliza para material en que los adultos participan en actos sexuales consentidos y que se distribuye legalmente al público en general para su placer sexual. Las imágenes de abuso infantil no lo son. Se trata de niños que no pueden dar su consentimiento ni lo darían y que son víctimas de un delito. De hecho, desde la perspectiva de la aplicación de la ley, el material que muestra abusos sexuales de niños es una prueba documentada del delito de abuso sexual o de violación en curso (UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, Nueva York, 2015, pág. 10).

situación en cuanto a las ratificaciones, así como por carecer de un enfoque integral y por el hecho de que no tenía en cuenta las tendencias actuales en el delito cibernético y no era plenamente adecuado para los países en desarrollo. Se señaló la atención sobre la resolución 74/247 de la Asamblea General, en la que esta había decidido establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Algunas delegaciones expresaron la opinión de que elaborar una convención de las Naciones Unidas facilitaría la eficiencia de la cooperación internacional en la lucha contra la ciberdelincuencia. Otras delegaciones expresaron la opinión de que los nuevos marcos o instrumentos en materia de ciberdelincuencia no deberían crear obstáculos ni hacer que los Estados abandonaran o contravinieran los tratados vigentes, los compromisos previamente adquiridos o los acuerdos alcanzados.

c) En las investigaciones de delitos cibernéticos es necesario contar con socios estratégicos, como por ejemplo, los miembros de organizaciones existentes tales como la Organización de los Estados Americanos (OEA), el Grupo de los 7 y la Organización Internacional de Policía Criminal (INTERPOL).

d) En investigaciones y procedimientos judiciales, debían respetarse la soberanía y la jurisdicción de los Estados. No debería solicitarse a empresas o particulares la entrega directa de datos ubicados en otro país sin el consentimiento previo de este.

e) Debería mejorarse la eficiencia de la cooperación internacional estableciendo mecanismos de respuesta rápida para la cooperación internacional, así como canales de comunicación entre las autoridades nacionales mediante oficiales de enlace y sistemas informáticos para la reunión trasfronteriza de pruebas y la transferencia en línea de pruebas electrónicas.

f) Los Estados deberían seguir estrechando la cooperación para proteger la infraestructura crítica y fortalecer las redes de colaboración entre los equipos informáticos de respuesta de emergencia y los equipos de respuesta a incidentes de ciberseguridad.

g) Los Estados deberían estudiar la posibilidad de crear protocolos innovadores de intercambio de información, incluidas la información de inteligencia y las pruebas de actos delictivos, a fin de agilizar esos procedimientos.

h) Es necesario reafirmar el compromiso de todos los Estados Miembros de garantizar la seguridad de las tecnologías de la información y las comunicaciones utilizándolas exclusivamente con fines pacíficos e intensificando las iniciativas internacionales para combatir las actividades malintencionadas en el ciberespacio en una época de profunda crisis en los planos mundial, regional y local.

i) Deberían optimizarse los procedimientos de cooperación internacional para que se preste la máxima asistencia dentro de las posibilidades que ofrezcan los marcos jurídicos nacionales a las solicitudes de cooperación internacional relativas a la conservación de pruebas electrónicas, y el acceso a archivos de conexión y la información de registro de los usuarios de un modo que no vulnere los derechos humanos, las libertades fundamentales o los derechos de propiedad.

j) Es necesario preparar un procedimiento operativo estándar, que sea aceptable internacionalmente, para la reunión y conservación de datos, y que pueda aplicarse en la escena de un delito. Es fundamental la adopción universal de prácticas internacionales estándar sobre la reunión, el almacenamiento y la compartición de pruebas, en particular en el proceso de investigación de delitos cibernéticos y el enjuiciamiento de ciberdelincuentes.

k) Se exhorta a los países a que presten especial atención a la necesaria proporcionalidad de las medidas de investigación, de modo que se respeten las libertades fundamentales y los regímenes de protección de datos personales asociados con la correspondencia privada.

l) La cooperación internacional en la lucha contra la ciberdelincuencia también debería tener en cuenta enfoques sensibles al género y la edad, así como las necesidades de los grupos vulnerables.

m) Los Estados deberían abstenerse de aplicar medidas unilaterales ilícitas que no estén en consonancia con el derecho internacional y con la Carta de las Naciones Unidas.

n) En cuanto al alcance de la cooperación internacional, si bien solo deberían prestar asistencia judicial recíproca las autoridades nacionales, la cooperación no debería circunscribirse a los departamentos gubernamentales, sino que también debería implicar al sector privado, por ejemplo, a los proveedores de servicios de Internet. En ese sentido, se recomendó la aprobación de disposiciones que permitieran entablar una cooperación directa con los proveedores de servicios de Internet de otras jurisdicciones con respecto a solicitudes de información sobre los abonados y solicitudes de conservación de datos.

o) Las opciones para combatir la ciberdelincuencia y proteger las sociedades deben salvaguardar siempre los derechos humanos y las garantías constitucionales, y promover un ciberespacio más libre, abierto, seguro y resiliente para todos.

p) Se alienta a los países a que simplifiquen la cooperación con el sector privado y a que refuercen la colaboración entre los Gobiernos y los proveedores de servicios privados, en particular para hacer frente a los retos que plantea la presencia de material delictivo nocivo en Internet.

q) Las empresas privadas, fundamentalmente los proveedores de servicios de Internet, tienen una responsabilidad compartida en la prevención e investigación del delito cibernético y deberían agilizar y ampliar sus respuestas a las solicitudes de asistencia judicial, ofrecerlas en los países en que estén establecidas y asegurarse de que disponen de los canales apropiados para comunicarse con las autoridades locales.

r) Deben reforzarse las alianzas entre los sectores público y privado. En los casos en que no existan esas alianzas, deben crearse, y las empresas privadas deberían participar en grupos de trabajo (foros multilaterales) y en el diálogo abierto para mejorar el enfoque que se sigue frente al delito cibernético.

s) Las organizaciones no gubernamentales y el mundo académico también deben implicarse en la labor de prevención y lucha contra la ciberdelincuencia, por cuanto aportan una perspectiva inclusiva, multifacética y amplia con la finalidad, entre otras, de garantizar la protección de los derechos humanos, especialmente la libertad de expresión y el derecho a la vida privada.

t) Se exhorta a los países a que, para conservar e intercambiar pruebas electrónicas admisibles, se incorporen a redes autorizadas de profesionales, como las redes que operan de manera ininterrumpida, las redes especializadas en ciberdelincuencia y los canales de INTERPOL para la cooperación interpolicial ágil, y a que utilicen esas redes en mayor medida y las refuercen; se exhorta también a los países a que establezcan redes con socios que tengan la misma estrategia, con vistas a intercambiar datos sobre asuntos de ciberdelincuencia, habilitar respuestas rápidas y minimizar la pérdida de pruebas esenciales. También se recomendó el uso de la cooperación interpolicial y otros métodos de cooperación oficiosa antes de acudir a los canales de asistencia judicial recíproca.

u) Cada Estado debería establecer un verdadero punto de contacto disponible de manera ininterrumpida, dotado de recursos suficientes, para facilitar la conservación de datos digitales, junto con la tradicional asistencia recíproca internacional en asuntos penales, tomando como punto de partida el modelo de éxito de la congelación de datos con arreglo al Convenio sobre la Ciberdelincuencia del Consejo de Europa.

v) Los Estados Miembros deberían intercambiar información sobre la forma en que se están resolviendo en el plano nacional los problemas para acceder de manera oportuna a las pruebas digitales, con el fin de que otros Estados Miembros se beneficien de esas experiencias y aumenten la eficiencia y eficacia de sus propios procesos.

w) Los Estados Miembros deberían establecer prácticas que permitan transmitir y recibir solicitudes de asistencia judicial recíproca por medios electrónicos, a fin de reducir las demoras en la transmisión de documentos de un Estado a otro.

x) Los países deberían fortalecer la colaboración interinstitucional y deberían mejorar la interoperabilidad estandarizando las solicitudes de información y los procedimientos de autenticación, y logrando la aceptación por parte de múltiples interesados.

y) Los países deberían mejorar la aplicación de las leyes nacionales y reforzar la coordinación y las sinergias a nivel interno para la reunión y el intercambio de información y pruebas con fines de enjuiciamiento.

z) Los Estados Miembros deberían establecer regímenes nacionales que hagan más rápida y eficiente la compartición de la "información sobre los abonados", según se define en el artículo 18, párrafo 3, del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

aa) Los Estados deberían fortalecer las medidas en lo que respecta al intercambio de información financiera o monetaria, la congelación de cuentas y el decomiso de bienes para garantizar que los delincuentes no puedan beneficiarse de las actividades delictivas.

bb) Se alienta a los Estados a que establezcan equipos conjuntos de investigación con otros países en los planos bilateral, regional o internacional para aumentar la capacidad de hacer cumplir la ley.

cc) Los Estados también deberían facilitar un tratamiento eficaz de las pruebas electrónicas y la admisibilidad de dichas pruebas ante los tribunales, incluso cuando se destinen a una jurisdicción extranjera o se reciban de ella. A ese respecto, se los alienta a que continúen o inicien reformas de la legislación sobre el delito cibernético y las pruebas electrónicas, siguiendo los ejemplos positivos y las reformas emprendidas en todo el mundo.

dd) Se recomienda elaborar marcos jurídicos que abarquen también los aspectos relacionados con la jurisdicción extraterritorial respecto de los actos de ciberdelincuencia.

ee) Los países deberían perfeccionar los mecanismos para mitigar los conflictos y hacer frente a las dificultades relacionadas con la atribución y la capacidad para investigar los casos de ciberdelincuencia.

ff) Los Estados deberían tratar de estandarizar y difundir instrumentos procesales para la aportación acelerada de datos y la ampliación de las búsquedas (como las órdenes de entrega de datos y las órdenes de medidas aceleradas de conservación o de acceso transfronterizo) a fin de facilitar la labor de las autoridades encargadas de hacer cumplir la ley y su cooperación directa con los proveedores de servicios de Internet y resolver los problemas relacionados con el rastreo de las pruebas electrónicas y su utilización adecuada.

gg) Los Estados deberían facilitar la elaboración y estandarización de normas técnicas interoperables para la labor forense digital y la recuperación de pruebas electrónicas transfronterizas.

hh) Se recomienda invertir en el establecimiento de una autoridad central sólida para la cooperación internacional en asuntos penales a fin de velar por la eficacia de los mecanismos de cooperación en lo que respecta al delito cibernético. También se recomienda establecer unidades específicas para investigar los delitos cibernéticos, así como atender las solicitudes de conservación de otros Estados mediante una red que funcione las 24 horas del día, los 7 días de la semana (o directamente con el proveedor en algunas circunstancias), a fin de preservar los datos necesarios lo más rápidamente

posible. Una mayor comprensión de la información que se necesita para que una solicitud de asistencia judicial recíproca sea admitida puede contribuir a que se obtengan los datos más rápidamente.

ii) Resultaría útil establecer un arreglo oficial con organizaciones como el Centro Europeo contra la Ciberdelincuencia de la Agencia de la Unión Europea para la Cooperación Policial (Europol), el Centro contra los Delitos Cibernéticos de los Estados Unidos de América, el Centro de Control del Delito Cibernético del Japón y el Centro Nacional de Seguridad Cibernética del Reino Unido de Gran Bretaña e Irlanda del Norte, con el fin de compartir información sobre las amenazas más recientes del delito cibernético, los *modus operandi*, la tecnología emergente para las investigaciones de delitos cibernéticos, así como para el acceso recíproco, las mejores prácticas, etc.

jj) Para que la cooperación internacional sea eficaz, es necesario que las leyes nacionales establezcan procedimientos que permitan la cooperación internacional. Por tanto, la legislación nacional debe posibilitar la cooperación internacional entre los organismos encargados de hacer cumplir la ley.

kk) Los Estados deberían llevar a cabo una cooperación eficaz en materia de extradición. Si un Estado requerido tiene la intención de negar la extradición de un sospechoso de un delito cibernético, debería, previa solicitud, hacer todo lo posible por consultar con el Estado requirente, a fin de dar al Estado requirente la oportunidad de expresar su opinión y proporcionar información. El Estado requerido debería comunicar los motivos de la denegación al Estado requirente.

ll) Más allá de las leyes nacionales, la cooperación internacional en materia de ciberdelincuencia se basa tanto en la cooperación oficial fundamentada en tratados como en la asistencia interpolicial tradicional. Al debatir sobre un nuevo instrumento relacionado con el delito cibernético, es importante que los países recuerden que un nuevo instrumento no debería entrar en conflicto con los instrumentos existentes, que ya hacen posible la cooperación internacional en tiempo real para muchos de ellos. Así pues, los países deberían procurar evitar todo conflicto entre cualquier instrumento nuevo contra el delito cibernético y los tratados existentes.

mm) Se debería priorizar y reforzar la creación de capacidad y la asistencia técnica sostenible para aumentar la capacidad en todas las esferas operacionales y fortalecer la capacidad de las autoridades nacionales para responder a la ciberdelincuencia, por ejemplo, mediante el establecimiento de redes, la celebración de reuniones y cursos de capacitación conjuntos, el intercambio de mejores prácticas, la facilitación de material de capacitación y la elaboración de plantillas para la cooperación. La creación de capacidad y la capacitación mencionadas deberían incluir una formación altamente especializada para los profesionales que promueva, en particular, la participación de mujeres expertas, y debería prestar atención a las necesidades de los legisladores y los encargados de formular políticas para tratar mejor las cuestiones relativas a la conservación de datos a efectos de hacer cumplir la ley. La creación de capacidad y la capacitación también deberían centrase en mejorar las habilidades de las autoridades encargadas de hacer cumplir la ley, los investigadores y los analistas en ciencia forense, en la utilización de datos de código abierto para las investigaciones, y en la cadena de custodia de las pruebas electrónicas, así como en la reunión y el intercambio de pruebas electrónicas en el extranjero. Otra esfera de prioridad en las actividades de creación de capacidad y capacitación debería ser la mejora de las habilidades de jueces, fiscales, autoridades centrales y abogados para juzgar y tratar eficazmente los casos pertinentes.

nn) Es esencial elaborar normas y plazos adecuados, y de ser posible uniformes, de retención y conservación de datos a fin de garantizar que puedan preservarse u obtenerse las pruebas electrónicas para respaldar nuevas solicitudes de asistencia judicial recíproca.

oo) La cooperación internacional es importante para reunir e intercambiar pruebas electrónicas en el contexto de las investigaciones transfronterizas y para responder rápida y eficazmente a las solicitudes de asistencia judicial recíproca relativas

a la conservación y la obtención de pruebas electrónicas. Durante el proceso deben respetarse los principios de soberanía y reciprocidad.

pp) Se alienta a la UNODC a que siga ofreciendo a los expertos gubernamentales nacionales programas de creación de capacidad y formación en la lucha contra la ciberdelincuencia, a fin de fortalecer la capacidad de detectar e investigar los delitos cibernéticos. Las actividades de creación de capacidad en esa esfera deberían tener en cuenta las necesidades de los países en desarrollo, centrarse en las vulnerabilidades de cada país a fin de prestar una asistencia técnica adaptada a sus circunstancias, y promover el intercambio de los conocimientos más actualizados en interés de los profesionales e interesados.

qq) La UNODC ha elaborado el Programa para Redactar Solicitudes de Asistencia Judicial Recíproca a fin de ayudar a los profesionales de la justicia penal a redactar dichas solicitudes. La Oficina también ha elaborado una guía práctica para la solicitud de pruebas electrónicas transfronterizas (*Practical Guide for Requesting Electronic Evidence Across Borders*), que está a disposición de los profesionales de los organismos de los Estados Miembros que la soliciten. Los países pueden beneficiarse de la utilización de esos instrumentos clave desarrollados por la UNODC.

rr) La Comisión de Prevención del Delito y Justicia Penal debería considerar la posibilidad de prorrogar el plan de trabajo del Grupo de Expertos más allá de 2021 como foro para que los profesionales intercambien información sobre el delito cibernético.

ss) Algunos oradores recomendaron que la negociación y aprobación de una convención de las Naciones Unidas para promover la cooperación en la lucha contra el delito cibernético facilitara una cooperación internacional más eficiente en la lucha contra la ciberdelincuencia.

tt) Se recomendó que fueran los expertos de la UNODC en Viena quienes se ocuparan de elaborar tal convención.

uu) Algunos oradores recomendaron que la Comisión de Prevención del Delito y Justicia Penal renovara el mandato del Grupo de Expertos y adoptara una decisión respecto de un plan de trabajo para después de 2021, que también debería incluir las formas emergentes de delitos cibernéticos y el examen de las cuestiones relacionadas con el abuso sexual de niños y la explotación infantil en Internet.

vv) Además, se recomendó que el comité intergubernamental especial de expertos de composición abierta, establecido en virtud de la resolución 74/247 de la Asamblea General a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, no iniciara su labor sino hasta después de que el Grupo de Expertos hubiera acordado sus recomendaciones y las hubiese enviado a la Comisión de Prevención del Delito y Justicia Penal en 2021.

ww) Sin embargo, otros oradores afirmaron que no era necesario que la labor del Grupo de Expertos continuara después de 2021, habida cuenta de la aprobación de la resolución 74/247 de la Asamblea General. Ello permitiría centrarse en la aplicación de esa resolución y en la negociación de una nueva convención, y aprovechar de la mejor manera los recursos disponibles.

xx) En sus declaraciones, los representantes de muchos Estados Miembros acogieron con beneplácito la aprobación de la resolución 74/247 de la Asamblea General. Se afirmó que la elaboración de la nueva convención de conformidad con esa resolución debía ser inclusiva y transparente y basarse en el consenso, y que los anteriores procesos de las Naciones Unidas para concertar la Convención contra la Delincuencia Organizada Transnacional y la Convención contra la Corrupción podían considerarse ejemplos en ese sentido.

yy) Se pidió la participación activa de todos los Estados Miembros en la labor del comité especial para elaborar una nueva convención.

zz) Al mismo tiempo, otros oradores afirmaron que, en lo que respecta al contenido, una nueva convención debería tener en cuenta los marcos e instrumentos existentes y no entrar en conflicto con ellos. Se recomendó que las cuestiones de la obtención transfronteriza de pruebas, las disposiciones en materia de penalización y el respeto de la soberanía se incluyeran en la posible nueva convención.

aaa) La comunidad internacional debería dar prioridad a la prestación de apoyo para la creación de capacidad y de otro tipo a fin de fortalecer la capacidad de las autoridades nacionales para responder al delito cibernético y, en particular, al abuso sexual de niños y la explotación infantil en Internet.

bbb) Los Estados Miembros deberían prestarse asistencia judicial recíproca para obtener pruebas electrónicas en la mayor medida posible, incluso en casos relacionados con el uso de las tecnologías de la información y las comunicaciones para cometer actos de terrorismo, incitar a su comisión o financiarlos; se afirmó además que las entidades del sector privado tenían la responsabilidad de cooperar con las autoridades nacionales a ese respecto.

ccc) Los Estados Miembros deberían considerar la posibilidad de invertir en fuerzas centralizadas especializadas en el delito cibernético y en dependencias tecnológicas regionales de investigación penal.

ddd) Los Estados Miembros también deberían considerar la posibilidad de establecer dependencias separadas para el delito cibernético dentro de las autoridades centrales para la asistencia judicial recíproca, a modo de base de conocimientos especializados en la compleja esfera de la cooperación internacional. Esas dependencias especializadas no solo aportan beneficios en la práctica cotidiana de la asistencia judicial recíproca, sino que también permiten prestar asistencia específica para el fomento de la capacidad, como por ejemplo, formación para atender a las necesidades de las autoridades nacionales y extranjeras sobre la forma de obtener de manera rápida y eficiente asistencia judicial recíproca que entrañe pruebas electrónicas, en cuestiones relacionadas con los delitos cibernéticos.

eee) Los Estados Miembros deberían considerar la posibilidad de mantener bases de datos electrónicas que faciliten el acceso a estadísticas relativas a las solicitudes entrantes y salientes de asistencia judicial recíproca que entrañen pruebas electrónicas, a fin de garantizar que se realicen exámenes de la eficiencia y la eficacia.

fff) Se debería recordar a los Estados Miembros que recurran a las autoridades centrales en la transmisión de solicitudes de asistencia judicial recíproca y en la colaboración con las autoridades competentes para la ejecución de dichas solicitudes, a fin de garantizar el cumplimiento de los tratados existentes y reducir las demoras en el proceso.

ggg) Para obtener datos que permitan realizar investigaciones relativas a actos de ciberdelincuencia, los Estados deberían aprovechar los instrumentos internacionales de probada eficacia, ya que esas investigaciones son complejas y requieren un marco institucional que haya demostrado su resistencia y valor añadido. A ese respecto, se puso de relieve el Convenio sobre la Ciberdelincuencia del Consejo de Europa, que ha servido de estándar para la obtención de pruebas electrónicas a lo largo de los años y que ha dado resultados a diario para los organismos encargados de hacer cumplir la ley de todo el mundo. Se recomendó que los Estados redujeran los conflictos de leyes en relación con los requisitos jurídicos aplicables teniendo en cuenta, como puntos de partida, en el caso de órdenes directas de presentación de datos, la legislación del Estado en que se encuentra el proveedor de servicios de Internet al que se solicita información o la del Estado del cual el sospechoso es ciudadano.

hhh) Se recomienda crear un marco en el que quede claro que, en caso de “pérdida de la ubicación”, la decisión de proceder con una investigación requiere un esfuerzo para establecer qué territorio ha sido afectado, dónde es vital la integridad de las redes automatizadas para poder realizar consultas sobre cuestiones de jurisdicción, y cuál es la forma más adecuada de continuar las indagaciones.

iii) Se recomendó que fuera aplicable en el ciberespacio el derecho internacional, incluidos los principios de soberanía, integridad territorial y no intervención en los asuntos internos, que no se emplearan las tecnologías de la información y las comunicaciones como armas y que se condenaran los ataques patrocinados por los Estados y se exigieran cuentas a los responsables.

jjj) Con sujeción a su derecho interno, el Estado requerido debería prestar la máxima asistencia a las solicitudes de investigación y reunión de pruebas que no afecten a la libertad personal o a los derechos de propiedad, o que tengan una repercusión mínima en esos derechos.

kkk) En la lucha contra el delito cibernético, los Estados deberían establecer un mecanismo y un canal de comunicación de respuesta rápida para la asistencia judicial y la cooperación en materia de aplicación de la ley, y considerar la posibilidad de permitir el intercambio en línea de documentos jurídicos y pruebas electrónicas, con el apoyo de firmas electrónicas y otros medios técnicos.

lll) La comunidad internacional debería formular un procedimiento unificado para las técnicas de investigación de los delitos cibernéticos y mejorar las disposiciones de su legislación interna relativas a las obligaciones de los proveedores de servicios de Internet de conservar registros.

mmm) Los Estados deberían impedir las transferencias internacionales del producto ilícito obtenido de los delitos cibernéticos y fortalecer la cooperación internacional en materia de recuperación de activos relacionados con el delito cibernético.

nnn) Los Estados deberían respetar la soberanía de otros Estados al establecer su jurisdicción sobre el delito cibernético y no deberían ejercer una jurisdicción extraterritorial excesiva que carezca de una relación suficiente y auténtica con el delito cibernético enjuiciado. Se alienta a los Estados a que mejoren la comunicación y las consultas para resolver los conflictos de jurisdicción.

ooo) Es importante velar por el uso seguro de las tecnologías de la información y las comunicaciones para proporcionar conectividad y sensibilización a todas las personas en todo el mundo, independientemente de la situación de los territorios en que residan los usuarios.

B. Prevención

14. De conformidad con el plan de trabajo del Grupo de Expertos, el presente párrafo contiene una recopilación, preparada por el Relator, de las sugerencias formuladas en la reunión por los Estados Miembros en relación con el tema 3 del programa, “Prevención”. Las recomendaciones y conclusiones preliminares fueron formuladas por los Estados Miembros, y su inclusión en el presente documento no supone que el Grupo de Expertos las haya hecho suyas; tampoco están presentadas en orden de importancia:

a) Debe reconocerse que la prevención no es solo responsabilidad de los Gobiernos: también requiere la participación de todos los interesados pertinentes, incluidos los organismos encargados de hacer cumplir la ley, el sector privado ─especialmente los proveedores de servicios de Internet─, las organizaciones no gubernamentales, las escuelas y los círculos académicos, además del público en general.

b) Se recomendó que el público tuviera fácil acceso a instrumentos de prevención como plataformas en línea, archivos de audio e infografías en lenguaje sencillo, y plataformas para presentar denuncias.

c) Se consideró necesario elaborar una serie de políticas públicas de largo plazo en materia de prevención, que deberían incluir el desarrollo de campañas de sensibilización sobre el uso seguro de Internet.

d) La sensibilización sobre la ciberseguridad debería incluirse como asignatura en la enseñanza primaria, secundaria y terciaria, tanto para los estudiantes como para los docentes. Lo ideal sería que esto formara parte de una estrategia nacional de ciberseguridad. Los Estados también deberían transmitir experiencias sobre la forma de utilizar las estrategias de ciberseguridad para prevenir el delito cibernético. Además, los Estados deberían prestar especial atención a las medidas de prevención dirigidas a los jóvenes, incluidos los que cometen delitos por primera vez, a fin de evitar la reincidencia.

e) Al prevenir y combatir el delito cibernético, los Estados deberían prestar especial atención a las cuestiones de la prevención y la erradicación de la violencia de género, en particular la violencia contra las mujeres y las niñas, y los delitos motivados por el odio.

f) Las actividades de prevención deben ser proactivas, periódicas, continuas y adecuadas para los grupos vulnerables.

g) La intersección y la colaboración entre los sectores público y privado con respecto a conjuntos o centros de macrodatos pueden representar un ámbito muy vulnerable, en particular, pero no exclusivamente, en el sector de la salud, tal como se ha visto durante la pandemia actual. Los Estados deberían prestar especial atención a la reglamentación del acceso legal a esos datos y a su protección contra ciberataques.

h) Con respecto a las medidas de prevención, los proveedores de servicios de Internet deberían asumir una mayor responsabilidad en cuanto a las precauciones de seguridad (“por defecto”) y la prevención del delito cibernético, y se deberían elaborar normas internacionales sobre el contenido y la duración de los registros que dichos proveedores de servicios de Internet deben conservar. Además, se deberían definir claramente las responsabilidades de los proveedores de servicios de Internet en lo que respecta a la detección, prevención y desbaratamiento del delito cibernético.

i) Se necesitan alianzas público-privadas para prevenir y combatir el delito cibernético, por ejemplo, iniciativas de cooperación con partes interesadas en la ciberseguridad y grandes empresas de tecnología en lo que respecta al intercambio de información.

j) Los Estados deberían impartir capacitación para magistrados y jueces especializados que se ocupan de los casos de delito cibernético, y proporcionar a los órganos de investigación instrumentos de alto rendimiento para rastrear las criptomonedas y hacer frente a su utilización con fines delictivos.

k) Los Estados deberían intensificar las estrategias para combatir el uso por parte de los grupos delictivos tradicionales de los instrumentos cibernéticos utilizados para ocultar sus comunicaciones y actividades.

l) Deberían elaborarse soluciones para la cooperación directa entre las autoridades nacionales y los proveedores de servicios de Internet, respetando al mismo tiempo el estado de derecho y los derechos humanos, incluidos los requisitos de protección de datos.

m) Los Estados deberían garantizar la libertad de prensa al elaborar medidas para prevenir el delito cibernético.

n) Se recomendó fomentar las capacidades colectivas de las instituciones competentes y cambiar la cultura de prevención de una reactiva a una proactiva. También se recomendó establecer un mecanismo sólido para estimular y facilitar el intercambio de información de inteligencia sobre los posibles *modus operandi* delictivos.

o) Se alienta a los Estados Miembros a que sigan incluyendo medidas de prevención eficaces en los planos nacional e internacional y a que se centren en actividades proactivas, como la sensibilización sobre los peligros del delito cibernético, realizando campañas relativas específicamente a los *modus operandi*, como el *phishing* o los programas maliciosos (“programas secuestradores”), y dirigidas a diferentes

grupos, como los jóvenes o las personas de edad. También se alienta a los Estados Miembros a que continúen centrándose en la probabilidad de enjuiciamiento y castigo de los delincuentes y los esfuerzos por prevenir el delito mediante la detección y el desbaratamiento de las actividades en curso de carácter ilícito en línea. Los servicios de policía y de fiscalía deberían invertir en detectar y señalizar las amenazas de la ciberdelincuencia y reaccionar a ellas. La colaboración entre el sector público y el privado es indispensable. Esas actividades de prevención no requieren leyes o reglamentos adicionales.

p) Debido a la existencia de la "brecha digital", algunos países en desarrollo carecen de capacidad para prevenir, detectar y combatir el delito cibernético, y son más vulnerables ante los desafíos que este plantea.

q) Se alentó encarecidamente a la UNODC a que siguiera prestando asistencia técnica, previa solicitud, para prevenir y combatir el delito cibernético.

r) Los futuros instrumentos internacionales de prevención del delito cibernético deberían ser accesibles a todas las personas en todo el mundo, sin distinción alguna por causa de la condición del país o territorio del que una persona sea nacional o residente.

s) Los derechos humanos básicos y las libertades fundamentales deberían protegerse en todas partes, incluso en el dominio digital y el ciberespacio, independientemente de las fronteras y sin ninguna interferencia ni limitación.

t) El ciberespacio y el delito cibernético no están limitados territorialmente y no reconocen ninguna frontera ni restricción física de otro tipo. Por tanto, la comunidad internacional debería permanecer unida para frenar las ciberamenazas.

u) El ciberespacio es una zona única y mundial y, a falta de un código de conducta internacional, deberían realizarse más esfuerzos para elaborar reglas, principios y normas de comportamiento responsable de los Estados en el ciberespacio. En ese contexto, todos los Estados Miembros deberían renunciar a la amenaza o al uso de la fuerza contra la infraestructura crítica de otros Estados.

v) Se alienta a los Estados Miembros a que sigan incluyendo medidas de prevención eficaces en los planos nacional e internacional y a que se centren en actividades proactivas, como la sensibilización sobre los peligros del delito cibernético y las probabilidades de que los delincuentes sean enjuiciados y castigados, e iniciativas para prevenir nuevos delitos mediante la detección e interrupción de las actividades ilícitas que se llevan a cabo en línea.

w) Las prácticas de ciberseguridad son distintas de los esfuerzos para combatir la ciberdelincuencia. Los Estados deberían elaborar tanto una estrategia nacional contra la ciberdelincuencia, que incluya legislación o una política nacional para la prevención de la ciberdelincuencia, como una estrategia nacional de ciberseguridad. Los ámbitos de acción de las estrategias nacionales contra la ciberdelincuencia deberían incluir la prevención de la ciberdelincuencia, alianzas público-privadas, la capacidad de la justicia penal y la sensibilización mediante la publicación de decisiones judiciales.

x) Los países deberían reunir una amplia gama de datos que ayuden a comprender las tendencias, a fin de fundamentar y configurar las políticas contra el delito cibernético y las respuestas operacionales para combatirlo.

y) Al elaborar estrategias de prevención del delito cibernético se debería tener en cuenta también la protección de los derechos humanos.

z) La "capacidad de la justicia penal" debería ser otra esfera de atención de las estrategias nacionales contra el delito cibernético. La asistencia a los países en desarrollo debería ser una prioridad, a fin de fortalecer la capacidad de los organismos encargados de cumplir la ley para prevenir el delito cibernético.

aa) Los Estados Miembros deberían aprovechar la asistencia para la creación de capacidad que prestan el Programa Mundial contra el Delito Cibernético de la UNODC y otras iniciativas, como los programas enmarcados en el proyecto Acción Global Ampliada contra la Ciberdelincuencia, del Consejo de Europa.

bb) Los Estados deberían establecer programas de apoyo a las víctimas de delitos cibernéticos, o reforzar los existentes.

cc) Los Estados deberían realizar estudios para medir los efectos del delito cibernético en las empresas, incluidas las medidas aplicadas, la capacitación de los empleados, los tipos de incidentes cibernéticos que les afectan y los costos relacionados con la recuperación tras los incidentes cibernéticos y su prevención.

dd) Los Estados deberían apoyar a las empresas y comunidades en la labor de concienciar sobre los riesgos del delito cibernético, adoptar estrategias de mitigación y mejorar las prácticas cibernéticas, ya que ello puede tener importantes beneficios en materia de prevención en el futuro.

ee) Se deberían estudiar atentamente los *modus operandi* de los ciberdelincuentes contemporáneos mediante el análisis de información de inteligencia y la investigación criminológica, a fin de asignar los recursos existentes de manera más eficaz y detectar las vulnerabilidades.

ff) Los Estados deberían considerar la posibilidad de establecer una plataforma de coordinación para promover el intercambio instantáneo de datos sobre incidentes y nuevas tendencias del delito cibernético que se hayan detectado. Los Estados también deberían considerar la posibilidad de establecer observatorios criminológicos para vigilar las amenazas y las tendencias del delito cibernético.

gg) Los países deberían considerar la posibilidad de adoptar medidas específicas y adaptadas para mantener a los niños seguros en línea. A tal fin, entre otras cosas, se debería velar por que los marcos jurídicos nacionales, los arreglos prácticos y los arreglos de cooperación internacional permitan la denuncia, detección, investigación, enjuiciamiento y disuasión del abuso y la explotación sexuales de los niños en Internet.

hh) La industria es un asociado clave en la prevención de la ciberdelincuencia. Los países deberían considerar la posibilidad de aplicar mecanismos de cooperación con la industria, incluso en lo que respecta a la remisión a las autoridades nacionales competentes y la retirada de material delictivo perjudicial, incluida la explotación sexual infantil y el material violento aborrecible.

ii) Periódicamente deberían publicarse y compartirse con usuarios, organizaciones y otras partes interesadas avisos sobre la prevención de incidentes, a fin de que estos puedan prevenir ciberincidentes que podrían dar lugar a actividades delictivas.

jj) Debería existir una metodología y procedimientos estándar para compartir información en vivo basada en pruebas con el fin de prevenir el delito cibernético.

kk) Debería elaborarse un mecanismo para registrar todos los servicios en línea y aplicar normas mínimas de referencia en materia de seguridad mediante reglamentación nacional.

ll) Los Estados deberían considerar la posibilidad de utilizar la inteligencia artificial para diseñar sistemas que se reconfiguren automáticamente ante un ataque.

mm) Se recomendó la creación de una base de datos mundial sobre los abusos relacionados con las criptomonedas y la explotación de datos por los delincuentes en gran escala, así como la elaboración de un panorama general estratégico, coordinado a nivel mundial, de las amenazas que plantean las infracciones penales cometidas en la Internet oscura.

nn) Deberían fomentarse las iniciativas regionales e internacionales destinadas a fortalecer la ciberseguridad, en particular, se debería fomentar el intercambio de información sobre ciberataques a gran escala.

oo) Los Estados tal vez deseen considerar la posibilidad de establecer un sistema internacional de comunicación de información sobre ciberamenazas destinado a compartir y estudiar las tecnologías y los *modus operandi* de las nuevas amenazas.

pp) Se alienta a los Estados a que establezcan un sistema de protección por niveles en materia de cibeseguridad para adoptar diferentes tecnologías de seguridad de la información y medidas de gestión para distintas instalaciones de información y comunicaciones, y a que velen por que la infraestructura crítica esté protegida frente al delito cibernético.

qq) Los Estados deberían implicar a mujeres expertas en la prevención e investigación de los delitos cibernéticos.

rr) Se deberían reunir experiencias nacionales y regionales de prevención para crear un repositorio multilateral que permita la difusión de buenas prácticas en diversos contextos.

ss) Se deben reforzar las medidas destinadas a prevenir la propagación del discurso de odio, el extremismo y el racismo.

tt) Se debería generar mayor conciencia acerca de los marcos reguladores contra el ciberacoso y las amenazas de violencia o abuso en línea, y se debería prestar asistencia legislativa al respecto.

uu) Se debería ofrecer creación de capacidad y cooperación para la prevención del delito cibernético con otros agentes y organizaciones regionales (como la OEA) y con foros de múltiples interesados, como el Foro Mundial de Competencia Cibernética.

vv) Se alienta a los Estados a que aprovechen la oportunidad de negociar una nueva convención sobre la lucha contra el delito cibernético para formular normas uniformes en la esfera de la prevención, a fin de coordinar las medidas de diversos países con mayor eficacia.

ww) Se recomendó que los Estados invirtieran en la creación de capacidad para mejorar las aptitudes de los funcionarios de todo el espectro del sistema de justicia penal, como medida preventiva eficiente de efecto disuasivo contra el delito cibernético.

xx) La UNODC debería facilitar la divulgación de mejores prácticas sobre medidas preventivas eficaces y satisfactorias contra el delito cibernético.

III. Resumen de las deliberaciones (resumen de la Presidencia)

15. A partir de la reunión y después de su celebración, la Secretaría preparó el siguiente resumen de las deliberaciones, en estrecha coordinación con el Presidente, de conformidad con la organización de los trabajos propuesta para la reunión, que se había comunicado a la Mesa ampliada del Grupo de Expertos el 13 de julio de 2020 y había sido aprobada por este en la apertura de la reunión. El resumen de las deliberaciones no fue objeto de discusión y, por consiguiente, tampoco se sometió a aprobación durante la reunión. Se trata de un resumen de la Presidencia, que figura a continuación, en las secciones A a C.

A. Cooperación internacional

16. En sus sesiones 1ª a 3ª, celebradas los días 27 y 28 de julio de 2020, el Grupo de Expertos examinó el tema 2 del programa, “Cooperación internacional”.

17. Facilitaron el debate los siguientes panelistas: George-Maria Tyendezwa (Nigeria), Gangqiang Zhang (China), Amornchai Leelakajonjit (Tailandia), Markko Künnapu (Estonia), Vadim Sushik (Federación de Rusia), Pedro Janices (Argentina), Stephen McGlynn (Australia) y Sheri L. Shepherd-Pratt (Estados Unidos).

18. Durante el debate, los oradores se refirieron al rápido aumento del delito cibernético, también a la luz de las dificultades que planteaba la pandemia de COVID-19, y destacaron la importancia de estrechar la cooperación internacional para hacer frente con eficacia al flagelo de los delitos basados en la cibernética y facilitados por ella, que eran de carácter transnacional y entrañaban un alto grado de complejidad delictiva y de

adaptación a las circunstancias y prioridades cambiantes. A ese respecto, muchos oradores hicieron referencia a medidas o reformas nacionales encaminadas a elaborar y aplicar estrategias y políticas de ciberseguridad; promulgar legislación sobre ciberdelincuencia o mejorar la ya existente; aplicar nuevos instrumentos de investigación para obtener pruebas electrónicas; y, sobre la base de sólidas medidas nacionales y de la mejora de las capacidades y la infraestructura, promover la cooperación internacional para combatir el delito cibernético.

19. Los oradores observaron que los problemas que planteaba la falta de armonización de las disposiciones relativas a la tipificación de los delitos, las lagunas en las facultades procesales de las autoridades de aplicación de la ley y de justicia penal, y los conflictos de jurisdicción al obtener pruebas electrónicas, requerían que los Estados Miembros renovaran su compromiso de lograr una cooperación regional e internacional eficaz y fortalecida para combatir el delito cibernético. A ese respecto, se resaltó que, si bien la cooperación internacional desempeñaba un papel fundamental en la lucha contra el delito cibernético y su prevención, se debía promover junto con los principios de soberanía, de respeto de las leyes nacionales y, a falta de un tratado aplicable, de reciprocidad, teniendo en cuenta también los diferentes niveles de capacidad y recursos de los Estados Miembros, especialmente de los países en desarrollo.

20. Se observó que, desde la anterior reunión del Grupo de Expertos, se habían producido novedades en la Tercera Comisión de la Asamblea General que habían añadido otra dimensión al debate internacional sobre el delito cibernético, a saber, la aprobación por la Asamblea de la resolución 74/247, en la que la Asamblea había decidido establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

21. Varios oradores expresaron la opinión de que la elaboración de una convención para combatir el delito cibernético en el marco de las Naciones Unidas facilitaría la eficiencia de la cooperación internacional en la esfera de la lucha contra el delito cibernético y sería la respuesta más adecuada al delito cibernético a nivel internacional. A ese respecto, recalcaron que un nuevo instrumento mundial contra el delito cibernético tendría en cuenta, entre otras cosas, las preocupaciones e intereses de todos los Estados Miembros, en particular los países en desarrollo, y contribuiría a colmar las lagunas jurídicas en esa esfera. Algunos de esos oradores reiteraron la opinión de que el Convenio sobre la Ciberdelincuencia del Consejo de Europa tenía un ámbito de aplicación limitado por su condición de instrumento regional y su situación en cuanto a las ratificaciones, así como por carecer de un enfoque integral, dado que no tenía en cuenta las tendencias actuales en el delito cibernético y no era plenamente adecuado para los países en desarrollo.

22. Otros oradores, no obstante, se mostraron partidarios de aprovechar al máximo los instrumentos o marcos y mecanismos internacionales existentes, como la Convención contra la Delincuencia Organizada, el Convenio sobre la Ciberdelincuencia del Consejo de Europa e INTERPOL. En lo que respecta a la Convención contra la Delincuencia Organizada, en particular, algunos oradores subrayaron que podía ser un instrumento muy útil para la cooperación internacional en la lucha contra el delito cibernético. Una oradora confirmó que su país había enviado y recibido numerosas solicitudes de asistencia basadas en las disposiciones de esa Convención como base jurídica para la cooperación internacional en materia de pruebas electrónicas en casos de ciberdelincuencia. Para apoyar aún más la utilización de ese instrumento, la oradora señaló que, en la mayoría de los casos importantes, el delito cibernético tenía su origen en alguna forma de delincuencia organizada, como las actividades en “mercados” clandestinos, con delincuentes en más de un país, y que los casos de delito cibernético en que intervenía un grupo delictivo organizado solían superar con creces los casos en que los piratas informáticos, actuando individualmente, eran los principales agentes delictivos.

23. Algunos oradores expresaron la opinión de que el Convenio sobre la Ciberdelincuencia del Consejo de Europa ofrecía un marco adecuado para elaborar respuestas apropiadas contra el delito cibernético a nivel nacional e internacional. Esos oradores recordaron que, con 65 Estados partes, de los cuales 21 no eran miembros del Consejo de Europa, el Convenio se utilizaba como base para una cooperación internacional eficiente, como modelo para la elaboración de legislación nacional y como norma para el fomento de la capacidad y la asistencia técnica. A su juicio, en el futuro previsible ese Convenio seguiría siendo el acuerdo multilateral más pertinente y progresista sobre el delito cibernético, ya que estaba a disposición de los países que buscaban una vía inmediata para introducir reformas legislativas sobre el delito cibernético, fortalecer su capacidad de aplicación de la ley y aumentar su cooperación internacional, todo ello sin perjuicio de las futuras deliberaciones sobre un nuevo instrumento en el marco de las Naciones Unidas. Un orador observó, no obstante, que el Convenio también tenía dificultades en relación con su aplicación deficiente en determinadas jurisdicciones y, por consiguiente, la elaboración de respuestas sobre la base de sus disposiciones se debía considerar como un proceso en constante evolución.

24. Se hizo referencia al proceso de negociación que se había puesto en marcha para aprobar un segundo protocolo adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa destinado a establecer normas claras y procedimientos más eficaces en relación con las siguientes esferas: disposiciones para entablar una cooperación internacional más rápida y eficaz; disposiciones que permitieran entablar una cooperación directa con proveedores de servicios de otras jurisdicciones respecto a solicitudes de información sobre los abonados, solicitudes de preservación de datos y solicitudes de emergencia; y un marco y unas salvaguardias estrictas respecto de las prácticas relativas al acceso transfronterizo a datos, con inclusión de requisitos de protección de datos.

25. Algunos oradores señalaron a la atención del Grupo de Expertos las experiencias en materia de cooperación internacional que habían surgido en el ámbito de organizaciones regionales, como la OEA, y de redes regionales, como la Comunidad de Policías de América, mientras que un orador mencionó que su país seguía colaborando estrechamente con la Organización Africana de Cooperación Policial (AFRIPOL) para combatir el delito cibernético.

26. Teniendo en cuenta las deliberaciones en curso relativas a llegar a un acuerdo sobre el esbozo y las modalidades de las actividades ulteriores del comité intergubernamental especial de expertos encargado de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, se destacó que la nueva convención debería orientarse a contener un enfoque inclusivo y alcanzar el mayor número posible de ratificaciones o adhesiones, siguiendo los ejemplos exitosos de la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción. También se hizo un llamamiento en favor de que el procedimiento de elaboración del instrumento fuera transparente, inclusivo y basado en el consenso, se fundamentara en las conclusiones y recomendaciones del Grupo de Expertos, y tuviera en cuenta los progresos que la comunidad internacional ya había realizado, así como la necesidad de promover una Internet libre, abierta y segura y proteger los derechos humanos en línea, lo cual incluía la protección de los datos personales y el derecho a la intimidad. Algunos oradores observaron que toda nueva convención debía elaborarse sobre la base del consenso y debía tener en cuenta los marcos e instrumentos existentes sin entrar en conflicto con ellos ni duplicarlos; no debía crear obstáculos ni hacer que los Estados abandonaran los compromisos asumidos previamente ni fueran en contra de ellos.

27. Algunos oradores observaron que, con los adelantos de la tecnología de la nube, una cantidad cada vez mayor de pruebas electrónicas se almacenaba en servidores fuera de la jurisdicción territorial de los Estados Miembros. Dado el carácter transnacional e inestable de esas pruebas electrónicas, se mencionó que la cooperación directa centrada principalmente en la comunicación de información de inteligencia era un instrumento muy útil para hacer frente a las limitaciones de tiempo y a los problemas que planteaban las circunstancias urgentes mediante la reducción del período necesario para activar los

canales de asistencia judicial recíproca. Se observó que la cooperación directa seguía basándose en la confianza mutua, pero que también se beneficiaría de la estandarización de las solicitudes y de la conservación acelerada de los datos, así como de la utilización más frecuente de los mecanismos ya existentes, como el sistema mundial de comunicación policial segura I-24/7 establecido por INTERPOL, y las redes de equipos de respuesta a incidentes de seguridad informática, tanto privadas como públicas. Además, podría resultar necesario crear protocolos innovadores para el intercambio de información y pruebas, a fin de agilizar esos procedimientos.

28. Se observó que una de las medidas clave en las investigaciones digitales y sobre delitos cibernéticos transfronterizas consistía en preservar la integridad de las pruebas electrónicas y velar por su autenticidad y su admisibilidad en las actuaciones penales conexas, para lo cual resultaban esenciales cuestiones como la cadena de custodia y las copias forenses. Desde esa perspectiva, se observó que debía darse prioridad al mejoramiento de las técnicas especiales de investigación, no solo para reunir pruebas electrónicas, incluso en la Internet oscura, sino también para realizar investigaciones financieras. A ese respecto, un orador señaló que las medidas para combatir el blanqueo de dinero y la financiación del terrorismo, así como las medidas de recuperación de activos, debían constituir una parte importante de la respuesta de los organismos de aplicación de la ley al delito cibernético. Otros oradores hicieron referencia a los problemas que planteaban las criptomonedas en la investigación y el enjuiciamiento de las corrientes ilícitas relacionadas con el producto del delito. Varios oradores resaltaron la necesidad e importancia de estudiar el modo de lograr que los profesionales de la justicia penal y las fuerzas del orden pudieran utilizar y sacar el máximo partido de las tecnologías en evolución, como la inteligencia artificial y las tecnologías de la información y las comunicaciones, incluidos los macrodatos, en la lucha contra la ciberdelincuencia.

29. En la esfera de la asistencia judicial recíproca, se determinó que la rápida ejecución de las solicitudes de asistencia judicial recíproca era una de las condiciones más importantes para que las medidas contra el delito cibernético y otros delitos que entrañaban pruebas electrónicas fueran eficaces. Algunos oradores mencionaron los factores que repercutían negativamente en la eficiencia de la asistencia judicial recíproca en la esfera del delito cibernético, entre ellos los diferentes requisitos legales y los distintos enfoques de tipificación que dificultaban el cumplimiento del requisito de la doble incriminación, así como la inexistencia de solicitudes con un contenido y un formato normalizados.

30. A fin de agilizar la cooperación internacional y racionalizar los procesos de asistencia judicial recíproca, se sugirió establecer un régimen separado para el acceso a la información sobre los abonados. En ese sentido, se observó que, en las deliberaciones en curso sobre el segundo protocolo adicional del Convenio sobre la Ciberdelincuencia del Consejo de Europa, se estaban estudiando medidas para obtener información sobre los abonados de manera más expedita.

31. Una oradora mencionó las medidas fundamentales que los países podían adoptar a fin de reducir el tiempo necesario para la ejecución de las solicitudes de asistencia judicial recíproca, como por ejemplo, la creación de capacidad y la capacitación sobre las necesidades específicas de cada país en materia de solicitudes de asistencia judicial recíproca, con objeto de reducir los plazos de respuesta y facilitar la ejecución de una solicitud sin necesidad de entablar largas comunicaciones adicionales para obtener más información; y el uso de canales de comunicación directos entre las autoridades centrales en lugar de los canales diplomáticos formales.

32. Algunos oradores subrayaron la necesidad de modernizar, racionalizar y agilizar la práctica de la asistencia judicial recíproca mediante la transmisión electrónica de las solicitudes de cooperación internacional, práctica que habían seguido recientemente algunos países iberoamericanos. A ese respecto, se sugirió que las autoridades centrales y otras autoridades competentes transmitieran, por correo electrónico, las solicitudes de asistencia, tanto oficiales como interinstitucionales, así como las solicitudes de conservación, utilizando redes que funcionaran de manera ininterrumpida.

33. Algunos oradores se refirieron al acceso transfronterizo a datos informáticos almacenados; recordaron que el Convenio sobre la Ciberdelincuencia del Consejo de Europa contenía una disposición específica al respecto (el artículo 32), y subrayaron que se debían aplicar cuidadosamente medidas conexas para equilibrar la necesidad de las investigaciones con la protección de los derechos humanos y la soberanía de los Estados.

34. Muchos oradores hicieron hincapié en la importancia de la creación de redes para mejorar la cooperación internacional en la lucha contra el delito cibernético. Se observó que las redes que funcionaban de manera ininterrumpida, con puntos de contacto responsables en cada país participante, desempeñaban un papel fundamental en la facilitación de la cooperación, en particular con respecto a las situaciones de emergencia. Esas redes, además, facilitaban las solicitudes de conservación de datos que a menudo eran objeto de una solicitud de asistencia judicial recíproca en una etapa posterior; normalmente esas solicitudes de conservación se tramitaban en días, o incluso en horas. Se reconoció en general que el riesgo que suponían las demoras en las investigaciones sobre delitos cibernéticos —ya que las pruebas podían borrarse rápidamente y los datos podían perderse o modificarse— hacía que resultara esencial pertenecer a una red que funcionara ininterrumpidamente o disponer de contactos con oficiales de enlace. Por esa razón, los oradores convinieron en que las autoridades centrales y otras autoridades competentes debían establecer relaciones y fortalecer aún más la confianza mutua mediante la comunicación y las consultas directas, y también mediante redes judiciales y policiales o redes especializadas en la lucha contra el delito cibernético de ámbito regional e internacional. Entre los ejemplos mencionados a ese respecto figuran la red de cooperación judicial en Asia Sudoriental (red SeaJUST), recientemente establecida; Cybernet (una red de la Asociación Iberoamericana de Ministerios Públicos (AIAMP), que reúne a puntos de contacto especializados de fiscalías y ministerios de todos los Estados miembros de la AIAMP); y la Red de Cooperación Penal de la AIAMP.

35. Algunos oradores opinaron que las estructuras o dependencias especializadas en delito cibernético de las autoridades centrales podían servir de base de conocimientos especializados en la compleja esfera de la cooperación internacional. Esas estructuras o dependencias especializadas podrían ofrecer los recursos y la experiencia necesarios para el funcionamiento cotidiano del régimen de asistencia judicial recíproca y podrían permitir también que se impartiera capacitación específica a autoridades nacionales y extranjeras sobre la forma de obtener asistencia y pruebas electrónicas de manera oportuna y eficiente en casos relacionados con la ciberdelincuencia.

36. Numerosos oradores resaltaron la importancia de fomentar y fortalecer la cooperación entre las autoridades nacionales y el sector privado, en particular con los proveedores de servicios de comunicaciones y los proveedores de servicios de Internet, a fin de mejorar la conservación de los datos y el acceso a ellos, y facilitar las respuestas prontas a la ciberdelincuencia, especialmente en casos transnacionales. Se sugirió crear un marco de referencia o una guía para facilitar un entendimiento común de los requisitos y procesos de ambas partes. Se subrayó que era necesario contar con disposiciones que permitieran entablar una cooperación directa con proveedores de servicios de otras jurisdicciones en relación con solicitudes de información sobre los abonados y solicitudes de preservación de datos. Se expresó la esperanza de que el segundo protocolo adicional del Convenio sobre la Ciberdelincuencia del Consejo de Europa, que se estaba negociando, ofreciera una solución más completa para la cooperación directa con entidades del sector privado.

37. Un orador recalcó que INTERPOL desempeñaba un papel único en la facilitación de la cooperación interpolicial, por conducto de las oficinas centrales de cada país, el sistema I-24/7 y sus notificaciones y bases de datos, y que el Programa Mundial de la INTERPOL sobre el Delito Cibernético, en particular, había desarrollado una plataforma de análisis cibernético y capacidades de colaboración para el intercambio de conocimientos y la coordinación operacional.

38. Muchos oradores consideraron necesaria, con carácter prioritario, la creación de capacidad sostenible en los organismos encargados de hacer cumplir la ley y los sistemas de justicia penal nacionales, lo cual incluía la creación de capacidad para los profesionales de las autoridades centrales que se ocupaban de la cooperación internacional. Se señaló que esas actividades de creación de capacidad eran esenciales, en particular para los países en desarrollo, desde el punto de vista de los recursos humanos, la infraestructura y el equipo, y con miras a superar la brecha digital que los separaba de los países desarrollados.

39. Hubo amplio acuerdo en que la creación de capacidad y la asistencia técnica basadas en los instrumentos existentes eran herramientas valiosas y eficaces en la lucha contra el delito cibernético y, por consiguiente, debían seguir desarrollándose y priorizándose, respetando al mismo tiempo las prioridades de los Estados Miembros. A ese respecto, varios oradores, como donantes o como receptores de asistencia, expresaron su apoyo al Programa Mundial contra el Delito Cibernético de la UNODC y a otros programas o marcos de asistencia técnica como, por ejemplo el programa de la INTERPOL, los programas enmarcados en el proyecto Acción Global Ampliada contra la Ciberdelincuencia, del Consejo de Europa, y el programa de ciberseguridad en el contexto de la Declaración de Boe sobre la Seguridad Regional, del Foro de las Islas del Pacífico.

40. En relación con el papel de la UNODC, muchos oradores se centraron en alentar a la Oficina a que siguiera ofreciendo a expertos competentes programas de fomento de la capacidad y de capacitación en materia de lucha contra el delito cibernético, con miras a fortalecer la capacidad nacional para detectar e investigar el delito cibernético y facilitar la difusión de mejores prácticas sobre medidas preventivas eficaces y acertadas contra el delito cibernético. En particular, se subrayó la necesidad de capacitar a los distintos actores de las esferas de la justicia penal y la aplicación de la ley, como jueces, fiscales y agentes de seguridad; la necesidad de crear y estructurar adecuadamente unidades especializadas para la investigación y el enjuiciamiento de los actos de ciberdelincuencia; y la necesidad de garantizar el acceso a las tecnologías más avanzadas para las investigaciones de delitos cibernéticos y con fines de ciencia forense digital. Algunos oradores afirmaron que las iniciativas de creación de capacidad en esos ámbitos deberían tener en cuenta las necesidades de los países en desarrollo, centrarse en las vulnerabilidades de cada país, para prestar una asistencia técnica adaptada a sus circunstancias, y promover el intercambio de los conocimientos más actualizados en interés de los profesionales e interesados.

41. Una oradora se refirió a la importancia de la capacitación de los funcionarios encargados de hacer cumplir la ley y a la labor realizada por la academia sobre ciberdelincuencia de la Agencia de la Unión Europea para la Formación Policial y la Academia Internacional para el Cumplimiento de la Ley. También se destacó la importancia de la cooperación internacional en el ámbito de la capacitación y la educación. Algunos oradores expresaron su apoyo a la prestación de capacitación a magistrados y jueces especializados que se ocupaban de casos de delito cibernético, así como su apoyo al suministro de instrumentos de alto rendimiento a los órganos de investigación para rastrear las criptomonedas y hacer frente a su utilización con fines delictivos.

42. Algunos oradores resaltaron innovaciones como la inclusión en el Programa para Redactar Solicitudes de Asistencia Judicial Recíproca de la UNODC, que se había rediseñado, de un módulo sobre pruebas electrónicas, que podía ayudar a racionalizar los procesos de asistencia judicial recíproca que entrañaban pruebas electrónicas. Asimismo, se mencionó la *Guía Práctica para la Solicitud de Pruebas Electrónicas Transfronterizas*, cuya elaboración formaba parte de la función de la UNODC de prestar asistencia técnica a los Estados Miembros.

43. Varios oradores subrayaron que los Estados Miembros debían abstenerse de adoptar medidas unilaterales ilegales que no estuvieran en consonancia con el derecho internacional y la Carta de las Naciones Unidas y que impidieran el pleno desarrollo económico y social de las poblaciones de los países afectados. Se afirmó que esas

medidas coercitivas unilaterales habían impedido la cooperación con fuerzas del orden nacionales en la investigación y el enjuiciamiento de delitos cometidos mediante la utilización de las tecnologías de la información y las comunicaciones, así como en la transferencia de los instrumentos tecnológicos necesarios para conservar las pruebas electrónicas y realizar exámenes forenses digitales.

44. Algunos oradores expresaron su preocupación por los ciberataques contra sectores de la infraestructura crítica, como el sector de la salud, llevados a cabo por algunos Estados Miembros o por grupos patrocinados por Estados, y destacaron que esos actos debían condenarse enérgicamente y las personas involucradas debían rendir cuentas. Otro orador expresó gran preocupación por el hecho de que la pandemia de COVID-19 había creado una nueva realidad para el sector de la salud, que se había convertido en blanco directo y víctima colateral de ataques contra la ciberseguridad, además de tener que enfrentar los abrumadores problemas de atención de la salud.

45. Algunos oradores expresaron la opinión de que la Comisión de Prevención del Delito y Justicia Penal debería considerar la posibilidad de prorrogar el plan de trabajo del Grupo de Expertos más allá de 2021 a fin de mantener un foro en el que expertos y profesionales pudieran intercambiar información sobre el delito cibernético, incluso a los efectos de examinar enfoques relativos al abuso y la explotación sexuales de niños en línea y otras formas emergentes de delito cibernético. Otros oradores subrayaron que, una vez terminado el plan de trabajo del Grupo de Expertos en su reunión de evaluación, que se celebraría en 2021, no había motivo para prorrogar su mandato, habida cuenta de la resolución 74/247 de la Asamblea General y de la necesidad de centrarse en la aplicación de esa resolución, la negociación de la nueva convención y la utilización óptima de los recursos disponibles.

46. Una oradora señaló que, aunque los mandatos del Grupo de Expertos y la resolución 74/247 de la Asamblea General eran diferentes, se debía centrar la atención en la convergencia y las complementariedades. En vista de ello, la cooperación internacional y el fomento de la capacidad, que habían sido promovidos por el Grupo de Expertos, debían reflejarse como pilares de la futura labor del comité especial encargado de negociar la nueva convención.

47. Otro orador recalcó que el comité especial debería comenzar su labor solo después de que el Grupo de Expertos hubiera concluido sus recomendaciones y las hubiera enviado a la Comisión de Prevención del Delito y Justicia Penal, en 2021.

B. Prevención

48. En sus sesiones 4ª y 5ª, celebradas los días 28 y 29 de julio de 2020, el Grupo de Expertos examinó el tema 3 del programa, “Prevención”.

49. Facilitaron el debate los siguientes panelistas: Destino Pedro (Angola), Liyun Han (China), Benjaporn Watcharavutthichai (Tailandia), Horacio Azzolin (Argentina), Claudio Peguero (República Dominicana) y Pedro Verdelho (Portugal).

50. Durante el debate se señaló que la prevención del delito cibernético se había convertido en un componente importante de las políticas y estrategias nacionales para prevenir y contrarrestar los ataques y amenazas cibernéticos, y disminuir las vulnerabilidades de la infraestructura cibernética y lograr una gestión eficaz de todos los riesgos conexos. La prevención del delito cibernético se examinó en el marco de un enfoque amplio de la lucha contra el delito cibernético que podría aplicarse en gran escala para que Internet y las tecnologías de comunicación conexas estuvieran siempre disponibles y fueran más seguras para los usuarios, y también para mejorar la cooperación, en todos los sectores y a todos los niveles, entre los agentes que participaban en esa labor en los planos nacional e internacional.

51. Varios oradores destacaron que los Estados Miembros, al elaborar estrategias de amplio alcance para la prevención del delito cibernético, debían tener presentes sus obligaciones internacionales en materia de derechos humanos. Una opinión de la que se hicieron eco otros oradores fue que la formulación de estrategias y propuestas

relacionadas con la prevención del delito cibernético debía basarse en una visión amplia que tuviera en cuenta los posibles efectos diferenciadores y asimétricos en los distintos grupos de población de un país, pero también en los distintos países, especialmente dada la brecha digital que existía entre los países desarrollados y los países en desarrollo y el hecho de que algunos países en desarrollo carecían de capacidad para prevenir, detectar y combatir el delito cibernético y eran más vulnerables a los problemas que este planteaba.

52. Se señaló que, en algunas jurisdicciones, la colaboración en materia de ciberseguridad era distinta de los programas de apoyo a las investigaciones de delitos cibernéticos y que, aunque a menudo se consideraban como las dos caras de la misma moneda, las políticas de aplicación de la ley contra el delito cibernético eran una responsabilidad exclusiva de los Gobiernos, mientras que la ciberseguridad era responsabilidad de diversos agentes públicos y privados. Además, se informó de que algunas organizaciones públicas y privadas seguían promoviendo la sensibilización en las empresas mediante programas destinados a mejorar las aptitudes en materia de ciberseguridad del personal informático.

53. Muchos oradores definieron las estrategias de interesados múltiples en materia de ciberdelincuencia como un elemento preventivo fundamental en la lucha contra ese tipo de delito. Se recalcó que las dificultades jurídicas, técnicas e institucionales que planteaba la ciberdelincuencia eran de gran alcance y solo podían abordarse aplicando estrategias coherentes e inclusivas basadas en iniciativas existentes y en la función de los distintos interesados. Desde esa perspectiva, se destacó la necesidad de promover y aumentar la participación de todos los agentes pertinentes en la prevención del delito cibernético y se señaló que las organizaciones regionales, el sector privado y los círculos académicos podían prestar un apoyo fundamental, en particular a los países en desarrollo, para lograr una cultura mundial de ciberseguridad.

54. Muchos oradores se hicieron eco de la necesidad de que las instituciones públicas ─como las autoridades de aplicación de la ley y de justicia penal─ y los proveedores de servicios de comunicaciones establecieran alianzas público-privadas basadas en la confianza mutua, en respuesta a los problemas multifacéticos con que se tropezaba en la lucha contra la ciberdelincuencia. Se hizo hincapié en la importancia de contar con buenas alianzas público-privadas, en particular en lo que respectaba a la detección y denuncia de delitos, la presentación de información sobre el paradero de los sospechosos y las víctimas, y la aportación de otros datos, según fuera necesario. Desde la perspectiva de las alianzas, también se hizo referencia a la necesidad de que los proveedores de servicios asumieran más responsabilidades adoptando precauciones de seguridad como medidas preventivas contra el delito cibernético. Esas responsabilidades deberían definirse claramente. También se subrayó que toda solución que se elaborara para la cooperación directa de las autoridades nacionales con los proveedores de servicios de Internet debía basarse en el estado de derecho y los derechos humanos y debía incluir requisitos de protección de datos.

55. Algunos oradores señalaron a la atención del Grupo de Expertos la responsabilidad, no solo de los Estados sino también de las empresas y otros agentes, en la protección de los datos, que permitía respetar el derecho a la intimidad, cuestión que, al igual que los derechos a la libertad de expresión y de prensa, se consideraba fundamental en la esfera de la prevención del delito cibernético. Se mencionó a la industria como un asociado clave en la prevención del delito cibernético que podría colaborar con las autoridades públicas en cuestiones como la remisión a las autoridades nacionales competentes y la retirada de material delictivo perjudicial, incluido el abuso sexual de niños y el material violento aborrecible.

56. Se resaltó el papel de las organizaciones no gubernamentales y de la comunidad académica en el contexto de estrategias inclusivas y amplias de prevención e investigación de la ciberdelincuencia que tuvieran en cuenta la protección de los derechos humanos, especialmente la libertad de expresión y la privacidad.

57. Muchos oradores se mostraron partidarios de que se adoptaran medidas de prevención eficaces en los planos nacional e internacional que incluyeran el enjuiciamiento y el castigo de los delincuentes, así como iniciativas para prevenir nuevos delitos mediante la detección e interrupción de las actividades ilícitas que se llevaban a cabo en línea. Se consideró que ese aspecto era un componente importante de las políticas preventivas debido a su efecto disuasorio, y se examinó junto con la necesidad de invertir en la creación de capacidad para mejorar las aptitudes de los funcionarios de todo el espectro del sistema de justicia penal, incluidas las mujeres expertas, a quienes se debería incluir a nivel nacional en la prevención e investigación del delito cibernético.

58. Como componente importante de las políticas de prevención de la ciberdelincuencia, se destacaron las campañas e iniciativas de sensibilización y educación, incluidas las relativas a las nuevas amenazas y las dirigidas a destinatarios concretos, como los niños. En ese contexto, se puso de relieve que debía darse prioridad al fomento de una "cultura de la ciberseguridad" a fin de que todos los agentes tuvieran mayor conciencia de los riesgos y amenazas delictivos que planteaba la ciberdelincuencia, y se llegara a un entendimiento común de las medidas de seguridad y prevención necesarias.

59. Se subrayó que la sensibilización sobre la ciberseguridad, en particular sobre los riesgos del delito cibernético y el lado oscuro de Internet, debería incluirse como asignatura en la enseñanza primaria, secundaria y terciaria, tanto para los estudiantes como para los docentes. Se añadió que lo ideal sería que ello formara parte de una estrategia nacional de ciberseguridad. Algunos oradores hicieron hincapié en la necesidad de prevenir la propagación del discurso de odio, el extremismo y el racismo, así como el ciberacoso y la violencia en línea, incluida la violencia de género y la violencia contra grupos vulnerables, ya fuera mediante iniciativas educativas, racionalizando los marcos regulatorios existentes, o ambas cosas. Además, un orador expresó la opinión de que los Estados debían prestar especial atención a las medidas de prevención dirigidas a las personas jóvenes, incluidos quienes cometían delitos por primera vez, a fin de evitar la reincidencia.

60. Un orador arrojó luz sobre la necesidad de contar con instrumentos que garantizaran la seguridad del comercio digital, y consideró que esa cuestión debía insertarse en una agenda de desarrollo más amplia para países que aún no se beneficiaban plenamente de esa forma de comerciar con bienes y servicios.

61. El análisis de inteligencia y la investigación criminológica se mencionaron como instrumentos importantes para prevenir la ciberdelincuencia. Se hizo referencia al análisis de grandes volúmenes de información de código abierto (ciberpatrullas) como método para detectar amenazas y vulnerabilidades, analizar su alcance y sus repercusiones y responder en una etapa temprana con alertas, guías y capacitación.

62. Un orador mencionó la labor de INTERPOL con asociados de los sectores público y privado para elaborar estrategias sólidas contra el delito cibernético, por ejemplo, mediante la realización de campañas mundiales de sensibilización destinadas a ayudar a las fuerzas del orden a superar los problemas que planteaba la lucha contra los delitos cibernéticos y el hecho de que se denunciaran menos delitos de los que realmente ocurrían.

63. Una oradora informó sobre la labor realizada en el marco del proyecto "No más rescates", iniciativa conjunta de organismos de aplicación de la ley y empresas de seguridad de la información y tecnológica que tenía por objeto perturbar las actividades ciberdelictivas relacionadas con programas secuestradores y ayudar a las víctimas de esos programas maliciosos a recuperar sus datos cifrados sin tener que pagar a los delincuentes. Esa misma oradora mencionó la Red Europea de Prevención de la Delincuencia, mediante la cual se difundían mejores prácticas en materia de políticas de ciberseguridad y protección.

C. Otros asuntos

64. En su sexta sesión, celebrada el 29 de julio de 2020, el Grupo de Expertos examinó el tema 4 del programa, “Otros asuntos”. No se planteó ninguna cuestión en relación con ese tema del programa.

IV. Organización de la reunión

A. Apertura de la reunión

65. Declaró abierta la reunión Doctor Mashabane (Sudáfrica), Presidente del Grupo de Expertos, quien delegó en André Rypl (Brasil), Vicepresidente del Grupo de Expertos, la presidencia de la reunión en su nombre.

B. Aprobación del programa y otras cuestiones de organización

66. En su primera sesión, celebrada el 27 de julio de 2020, el Grupo de Expertos aprobó el siguiente programa provisional:

1. Cuestiones de organización:
   a) Apertura de la reunión;
   b) Aprobación del programa.
2. Cooperación internacional.
3. Prevención.
4. Otros asuntos.
5. Aprobación del informe.

C. Declaraciones

67. Formularon declaraciones expertos de los siguientes Estados Miembros: Alemania, Argelia, Argentina, Armenia, Australia, Austria, Azerbaiyán, Brasil, Canadá, Chile, China, Colombia, Cuba, Ecuador, Egipto, España, Estados Unidos, Estonia, Federación de Rusia, Filipinas, Francia, Grecia, Guatemala, Honduras, Hungría, India, Indonesia, Irán (República Islámica del), Iraq, Israel, Italia, Japón, Líbano, Malasia, México, Mongolia, Nigeria, Noruega, Nueva Zelandia, Países Bajos, Paraguay, Perú, Polonia, Portugal, Reino Unido, República Dominicana, Rumania, Sudáfrica, Tailandia, Venezuela (República Bolivariana de) y Viet Nam.

68. Una experta del Estado de Palestina, Estado observador no miembro, formuló una declaración[2].

69. Formularon declaraciones también representantes de las siguientes organizaciones intergubernamentales: Consejo de Europa, INTERPOL y Unión Europea. Un observador de la Universidad Normal de Beijing hizo una declaración.

D. Asistencia

70. Asistieron a la reunión representantes de 93 Estados Miembros, un Estado observador no miembro, un instituto de la red del programa de las Naciones Unidas en materia de prevención del delito y justicia penal, organizaciones intergubernamentales y el sector privado.

[2] La observadora del Estado de Palestina también formuló una declaración en nombre del Grupo de los 77 y China.

71. En la reunión se distribuyó una lista provisional de participantes (UNODC/CCPCJ/EG.4/2020/INF/1).

E. Documentación

72. El Grupo de Expertos tuvo ante sí las observaciones de los Estados Miembros recibidas de conformidad con el plan de trabajo para el período 2018-2021, así como el programa provisional anotado (UNODC/CCPCJ/EG.4/2020/1).

V. Aprobación del informe

73. En su sexta sesión, celebrada el 29 de julio de 2020, el Grupo de Expertos aprobó el presente informe.