Naciones Unidas A/AC.292/2024/2

Asamblea General

Distr. general
22 de enero de 2024
Español
Original: inglés

Grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025)
Séptimo período de sesiones sustantivo
Nueva York, 4 a 8 de marzo de 2024

Análisis para estudiar el panorama de los programas e iniciativas de creación de capacidad dentro y fuera de las Naciones Unidas y a escala mundial y regional

Documento de la Secretaría

I. Introducción

1. En el párrafo 46 del informe sobre los progresos realizados en los debates del grupo de trabajo sobre el tema 5 del programa, que figura en el anexo del documento titulado “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional” (A/78/265), se pidió a la Secretaría de las Naciones Unidas que llevara a cabo un análisis, en consulta con las entidades pertinentes, con el fin de estudiar el panorama de los programas e iniciativas de creación de capacidad dentro y fuera de las Naciones Unidas y a escala mundial y regional, recabando entre otras cosas la opinión de los Estados Miembros. Además, se pedía a la Secretaría que elaborase un informe con las conclusiones de este análisis y que lo presentase en el séptimo período de sesiones del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), que se celebrará del 4 al 8 de marzo de 2024, como apoyo a las labores de los Estados por hacer balance de los esfuerzos existentes en materia de creación de capacidad y fomentar nuevas sinergias y coordinación entre estos esfuerzos. Este informe se presenta en cumplimiento de esa solicitud.

2. El 2 de octubre de 2023, la Oficina de Asuntos de Desarme distribuyó una nota verbal a todas las Misiones Permanentes ante las Naciones Unidas en la que se señalaba a su atención el párrafo 46 del informe mencionado y se las invitaba a expresar su opinión sobre el panorama de los programas e iniciativas de creación de capacidad en materia de tecnologías de la información y las comunicaciones dentro y fuera de las Naciones Unidas y a escala mundial y regional. El plazo de respuesta se fijó en el 10 de noviembre de 2023 y después se prorrogó hasta el 16 de noviembre. Al 22 de enero de 2024 habían presentado sus opiniones los siguientes Estados:

Alemania, Australia, Bélgica, Brasil, Burkina Faso, Camboya, Chequia, Chile, Colombia, Cuba, Eslovaquia, Eslovenia, Estados Unidos de América, Estonia, Federación de Rusia, Francia, India, Irán (República Islámica del), Líbano, México, Países Bajos (Reino de los), Portugal, Qatar, Reino Unido de Gran Bretaña e Irlanda del Norte, República de Corea, Singapur, Suiza, Türkiye y Uruguay.

3. La Oficina de Asuntos de Desarme solicitó además la opinión de las entidades pertinentes del sistema de las Naciones Unidas mediante cartas de fecha 2 de octubre de 2023. Al 22 de enero de 2024 habían presentado sus opiniones las siguientes entidades de las Naciones Unidas: Unión Internacional de Telecomunicaciones, Dirección Ejecutiva del Comité contra el Terrorismo, Programa de las Naciones Unidas para el Desarrollo, Instituto de las Naciones Unidas de Investigación sobre el Desarme, Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia, Oficina de Lucha contra el Terrorismo, Oficina de Tecnología de la Información y las Comunicaciones, Oficina de Asuntos Jurídicos y Oficina de las Naciones Unidas contra la Droga y el Delito.

4. Asimismo, el 2 de octubre de 2023 solicitó por correo electrónico aportaciones a las entidades no gubernamentales interesadas pertinentes. Al 22 de enero de 2024 habían presentado sus opiniones las siguientes entidades interesadas: Asociación para el Progreso de las Comunicaciones, Centro de Gobernanza de las Comunicaciones de la Universidad Nacional de Derecho de Dehli, DiploFoundation, Foro Mundial de Competencia Cibernética, Cámara de Comercio Internacional, Centro de Excelencia de Seguridad Nacional de la Escuela de Estudios Internacionales S. Rajaratnam, SafePC Solutions, Third Eye Legal y Write Pilot. La Unión Europea también envió sus opiniones. También se recibieron las siguientes comunicaciones conjuntas: una de la Argentina, el Brasil, Chile, Colombia, Costa Rica, el Ecuador, El Salvador, Guatemala, el Paraguay, la República Dominicana y el Uruguay, y otra de la Agencia Nacional Checa de Seguridad Cibernética y de la Información, el Comité Internacional de la Cruz Roja (CICR), el Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN), la Universidad de Exeter, United States Naval War College y la Universidad de Wuhan.

5. Todas las opiniones, incluidas las recibidas una vez concluida la prórroga del plazo oficial, pueden consultarse en el sitio web del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025)[1]. Se anima a los Estados a consultar en su totalidad las comunicaciones facilitadas por los Estados Miembros, las entidades del sistema de las Naciones Unidas y las entidades interesadas no gubernamentales, ya que este informe no representa un inventario exhaustivo de todas las actividades recogidas en ellas.

6. El presente informe se basa principalmente en la información recibida de los Estados Miembros, las entidades del sistema de las Naciones Unidas y las entidades no gubernamentales interesadas, sin perjuicio de la postura de cada uno de ellos. Se facilita asimismo información adicional procedente de fuentes abiertas con el fin de ofrecer un panorama equilibrado e ilustrativo de los programas e iniciativas de capacitación existentes dentro y fuera de las Naciones Unidas y a escala mundial y regional.

7. Se presentan ejemplos de programas e iniciativas de creación de capacidad, destacando en primer lugar los esfuerzos a escala regional y subregional, seguidos de información clasificada por temas generales. Estas descripciones no representan una reseña exhaustiva de todas las iniciativas y programas, sino que pretenden ofrecer un

[1] Se pueden consultar en https://meetings.unoda.org/meeting/57871/documents.

panorama general e ilustrativo de las actividades. Tampoco debe entenderse que haya ninguna priorización o clasificación de las actividades.

8. Al final del informe se presentan las observaciones y conclusiones de la Secretaría para ayudar a los Estados a llevar adelante iniciativas de creación de capacidad más eficaces, sostenibles y eficientes a escala mundial, regional y subregional.

II. Panorama de los debates y conclusiones de los Estados sobre la creación de capacidad a escala multilateral

9. A la luz de la evolución del panorama de las amenazas que se derivan del uso por parte de los Estados de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, los Estados siguen subrayando que es urgente mejorar la capacidad de todos los Estados de observar y aplicar el marco acumulativo y evolutivo de comportamiento responsable de los Estados, como se afirma en el segundo informe anual del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) (A/78/265).

10. Los Estados han destacado la necesidad de promover una mejor comprensión de las necesidades de los Estados en desarrollo con el objetivo de reducir la brecha digital a través de esfuerzos de creación de capacidad adaptados. También han subrayado la acuciante necesidad de crear capacidad y buenas prácticas en una serie de ámbitos diplomáticos, jurídicos, políticos, legislativos y normativos, así como de disponer de competencias técnicas, fortalecer las instituciones y recurrir a mecanismos de cooperación. Han insistido asimismo en el valor de la cooperación Sur-Sur, triangular y subregional y regional como complemento de la cooperación Norte-Sur y recordado el valor que tiene el enfoque de formación de formadores al establecer programas de formación especializada y de certificación profesional adaptados, a fin de poder transmitir los conocimientos y aptitudes necesarios a los homólogos pertinentes.

11. En el marco del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), los Estados siguen formulando propuestas concretas y orientadas a la acción sobre los esfuerzos de creación de capacidad, ejemplos de lo cual son una propuesta para desarrollar un portal mundial de cooperación en materia de ciberseguridad, una propuesta para fomentar un mayor intercambio técnico sobre las amenazas de las tecnologías de la información y de las comunicaciones para identificar y detectar actividades maliciosas y facilitar respuestas fundamentadas a ellas, y una propuesta para celebrar debates sobre el fomento de una participación significativa y de alianzas con partes interesadas no gubernamentales en el ámbito de la creación de capacidad, también con fines de formación e investigación.

12. El propio grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) ha sido reconocido como plataforma para seguir intercambiando opiniones e ideas relacionadas con los esfuerzos de creación de capacidad, incluida la mejor manera de aprovechar las iniciativas existentes con el fin de ayudar a los Estados a desarrollar la fuerza institucional necesaria para aplicar el marco de comportamiento responsable de los Estados.

13. En relación con el uso que hacen de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, los Estados han seguido promoviendo la incorporación de los principios de la creación de capacidad que

figuran en el anexo C del documento A/78/265, que se desarrollaron por primera vez en el informe final del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional[2]. Al respaldar estos principios, los Estados han llegado a la conclusión de que la creación de capacidad debe ser un proceso sostenible, integrado por actividades específicas basadas en resultados, y tener además un propósito claro, contar con una base empírica y ser políticamente neutro, transparente, responsable e incondicional. Además, los Estados han acordado que la creación de capacidad debe llevarse a cabo respetando plenamente el principio de la soberanía de los Estados, basarse en la demanda, corresponder a unas necesidades y prioridades determinadas a nivel nacional y respetar los derechos humanos y las libertades fundamentales. En su segundo informe (A/78/265), el grupo de trabajo recomendó que los Estados confeccionaran y compartieran listas de comprobación voluntarias y otras herramientas para integrar la aplicación de los principios acordados de creación de capacidad.

14. A través de los debates del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), los Estados han seguido concienciando sobre la dimensión de género de la seguridad en el uso de las tecnologías de la información y las comunicaciones y promoviendo la creación de capacidad con perspectiva de género a nivel normativo, así como en la selección y puesta en marcha de proyectos de creación de capacidad. También han alentado los esfuerzos encaminados a promover la creación de capacidad que responda a las cuestiones de género, por ejemplo mediante la integración de una perspectiva de género en las políticas nacionales de tecnologías de la información y las comunicaciones y en las iniciativas de creación de capacidad, así como mediante la elaboración de listas de comprobación o cuestionarios para determinar las necesidades y lagunas en este ámbito.

15. Los Estados han argumentado que las Naciones Unidas podrían ser esenciales para coordinar los esfuerzos de creación de capacidad, ya que pueden hacer balance de las necesidades de los Estados, determinar las lagunas existentes mediante herramientas y encuestas y facilitar el acceso de los Estados a programas de creación de capacidad, entre otras cosas mediante el presente análisis.

III. Cooperación regional, subregional e interregional

16. Los Estados han reafirmado sistemáticamente que las organizaciones regionales y subregionales desempeñan un papel importante en el apoyo a la aplicación del marco de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones, por ejemplo respaldando iniciativas de creación de capacidad conexas. Además, han reflexionado sobre los esfuerzos que se podrían emprender a escala regional, subregional e interregional, como talleres, cursos de formación e intercambios sobre mejores prácticas y lecciones aprendidas. Se ha alentado asimismo a los Estados a que apoyen los programas de creación de capacidad, incluso en colaboración, cuando proceda, con las organizaciones regionales y subregionales[3].

17. Por lo que respecta a la cooperación interregional, el Foro Mundial de Competencia Cibernética es una comunidad multipartita que cuenta con más de 200 miembros y asociados, tales como Estados de todas las regiones, organizaciones internacionales y regionales y actores del sector privado, la sociedad civil y el mundo

[2] A/75/816, anexo I, párr. 56.
[3] A/78/265, anexo, párr. 51.

académico. El portal Cybil, iniciativa emblemática del Foro, es un repositorio en línea de proyectos internacionales de capacitación cibernética y alberga una biblioteca de recursos para las partes interesadas[4].

18. En noviembre de 2023 el Foro Mundial de Competencia Cibernética organizó, en cooperación con Ghana, el Foro Económico Mundial, el Banco Mundial y CyberPeace Institute, la primera Conferencia Global sobre Creación de Capacidad Cibernética, que constó de varias sesiones regionales temáticas y de profundización y culminó en un documento final, el Llamamiento de Accra al Desarrollo Ciberresiliente, que comprende una serie de medidas orientativas, voluntarias y no vinculantes cuyo fin es: a) reforzar el papel de la ciberresiliencia como factor facilitador del desarrollo sostenible; b) fomentar la creación de cibercapacidad sostenible, eficaz y basada en la demanda; c) promover unas alianzas más fuertes y una mejor coordinación; y d) movilizar recursos financieros y modalidades de implementación[5]. En el marco de la Conferencia se anunció que la siguiente edición se celebrará en Ginebra en mayo de 2025 con el objetivo de ampliar los avances iniciados en Ghana.

19. A fin de reforzar la cooperación entre las regiones, la Alianza Digital Unión Europea-América Latina y el Caribe organiza diálogos sobre regulación y ciberseguridad, entre otras actividades sobre temas digitales y espaciales. Tiene como objetivo apoyar la transformación y la innovación digitales concibiendo las sociedades y economías digitales desde una perspectiva centrada en las personas. Para ello ha establecido un diálogo birregional sobre políticas digitales, ha ampliado el programa Construyendo el Vínculo de Europa con América Latina y el Caribe, ha implantado la estrategia regional Copernicus, encaminada a mejorar la resiliencia digital fomentando la capacidad de gestión de los datos especiales y su uso estratégico, y ha creado el Acelerador Digital Unión Europea-América Latina y el Caribe, cuyo fin es impulsar el emprendimiento y la innovación.

20. El proyecto en curso “Mejorar la cooperación en materia de seguridad en y con Asia”, respaldado por la Unión Europea y financiado por Alemania y Francia, tiene como finalidad aumentar la convergencia en cuanto a las políticas y las prácticas entre la Unión Europea y los países asociados, crear conciencia y apoyar diálogos sobre seguridad operacional[6]. En el marco de este proyecto se llevan a cabo actividades de cuatro esferas temáticas, a saber: lucha antiterrorista y prevención del extremismo violento, ciberseguridad, seguridad marítima y gestión de crisis. En la actualidad participan en él la India, Indonesia, el Japón, la República de Corea, Singapur y Viet Nam.

21. En la región de Europa Central y Oriental, Eslovenia, Francia y Montenegro pusieron en marcha en mayo de 2023 el Centro de Cibercapacidad de los Balcanes Occidentales[7], cuyo objetivo es ayudar a los seis países y zonas participantes a reforzar la cibercapacidad institucional y operacional. Entre otras cosas organiza cursos de capacitación, ha elaborado cibercurrículos y facilita el intercambio de información y mejores prácticas para ayudar a los especialistas de los Estados de los Balcanes Occidentales a prevenir ciberamenazas, prepararse para ellas y responder a ellas. En 2023 el Centro organizó cursos de capacitación sobre ciberhigiene para administraciones públicas, un programa de mentorías para mujeres sobre formulación de políticas y negociaciones internacionales en el ámbito cibernético, cursos sobre ciberdelincuencia para autoridades judiciales y fuerzas de policía y un curso sobre

[4] Véase https://cybilportal.org/about-cybil/.

[5] Se puede consultar en https://gc3b.org/news/read-the-full-accra-call-for-cyber-resilient-development/.

[6] Véase https://www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf.

[7] Véase https://cybilportal.org/projects/western-balkans-cyber-capacity-centre-wb3c/.

infraestructura crítica para oficiales principales de seguridad de la información. En el momento de redactar el presente documento estaban previstos 12 cursos de capacitación para 2024. Paralelamente, existe un proyecto de la Unión Europea dirigido por Chequia y Estonia cuya finalidad es apoyar la creación de ciberseguridad en los Balcanes Occidentales mediante: a) el desarrollo de la gobernanza de la ciberseguridad y la concienciación al respecto; b) el fortalecimiento de los marcos jurídicos, las cibernormas y el cumplimiento del derecho internacional; c) el desarrollo de la gestión de riesgos y crisis; y d) el refuerzo de las capacidades operacionales, en particular del equipo de respuesta a incidentes de seguridad informática. A los efectos de aumentar la resiliencia frente a los ciberincidentes se implementó también otro proyecto de la Unión Europea, titulado “Respuesta rápida en materia de ciberseguridad para Albania, Macedonia del Norte y Montenegro”.

22. El Departamento de Amenazas Transnacionales de la Organización para la Seguridad y la Cooperación en Europa (OSCE) lleva a cabo actividades para mejorar la capacidad de los Estados participantes de afrontar amenazas relacionadas con la seguridad en el marco de las tecnologías de la información y las comunicaciones. Entre tales actividades cabe destacar ejercicios para promover una respuesta nacional adecuada a los incidentes relacionados con infraestructura crítica, talleres sobre cómo contrarrestar el uso de Internet con fines terroristas y cursos de capacitación sobre la investigación y el enjuiciamiento de los delitos cibernéticos [8]. En 2023 el Departamento organizó en Viena un curso de capacitación sobre ciberdiplomacia internacional centrado en la creación de capacidad nacional para participar en deliberaciones internacionales sobre ciberpolítica. En cuanto que entidad a cargo de las escalas de gravedad y medidas conexas de los ciberincidentes nacionales para proteger las infraestructuras críticas, la OSCE contribuye a la elaboración de procedimientos de comunicación y gestión de crisis y métodos de clasificación de incidentes entre países de Europa, Asia Central y otras regiones. Además, actúa como foro multilateral para diversas discusiones sobre cibercooperación y creación de cibercapacidad.

23. La Federación de Rusia celebra seminarios y talleres en línea anuales con el Foro Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN) sobre terminología del ámbito de la seguridad de las tecnologías de la información y las comunicaciones y de su uso, la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y el desarrollo sostenible y seguro de Internet y criminalística digital. También ha organizado cursos de capacitación sobre la investigación de delitos de malversación relacionados con las tecnologías de la información y las comunicaciones en la Conferencia sobre Interacción y Medidas de Fomento de la Confianza en Asia.

24. La Unión Internacional de Telecomunicaciones (UIT), en cooperación con la Alianza Internacional Multilateral contra las Ciberamenazas, creó con el apoyo de Omán el Centro Regional de Ciberseguridad Omán-UIT[9], el cual, radicado en la sede del equipo de respuesta a emergencias informáticas de Omán, tiene como finalidad mejorar las capacidades, la preparación, las aptitudes y los conocimientos en los ámbitos de la ciberseguridad, la protección de infraestructura crítica y la creación de capacidad en la región árabe.

25. El Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA), por conducto de su Programa de Ciberseguridad, ayuda a los Estados Miembros a desarrollar sus capacidades técnicas, políticas y diplomáticas para prevenir y detectar ciberincidentes, responder a ellos y recuperarse

[8] Véase https://www.osce.org/secretariat/cyber-ict-security.

[9] Véase https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.aspx.

tras ellos y para promover el comportamiento responsable de los Estados en el ciberespacio[10]. Entre otras cosas, el Programa ayuda a elaborar estrategias nacionales de ciberseguridad y a crear equipos nacionales de respuesta a incidentes de seguridad informática. También proporciona asistencia y capacitación y guías a las instancias normativas, la industria y la sociedad civil y administra la red hemisférica de equipos de respuesta a incidentes de seguridad informática de América, que comparte información sobre amenazas e información de inteligencia entre 29 equipos de 20 Estados miembros de la OEA. El Programa también facilita una mayor transversalización de la perspectiva de género en la formulación de políticas sobre ciberseguridad y una mayor representación en los procesos multilaterales.

26. En octubre de 2023 se celebró en el Brasil el Foro Iberoamericano de Ciberdefensa[11], que contó con la participación de 13 Estados y tuvo como finalidad profundizar la integración y la cooperación regionales para prevenir, detectar y afrontar ciberamenazas. En él se llevaron a cabo, entre otras actividades, simulacros, como el ejercicio Cyber Guardian 5.0, y se desarrolló una plataforma de intercambio de información sobre *malware*.

IV. Panorama ilustrativo y no exhaustivo de las iniciativas de creación de capacidad por esfera temática

Derecho internacional

27. Los Estados han reconocido que son particularmente necesarias iniciativas de creación de capacidad sobre derecho internacional en el contexto de la seguridad de las tecnologías de la información y las comunicaciones. Han recalcado que es urgente proseguir tales esfuerzos de creación de capacidad, entre otras cosas para lograr que todos los Estados puedan participar en igualdad de condiciones en el desarrollo de un entendimiento común sobre cómo corresponde aplicar el derecho internacional en el uso de las tecnologías de la información y las comunicaciones. Entre dichos esfuerzos cabe señalar talleres, cursos de capacitación e intercambios de mejores prácticas a escala internacional, interregional, regional y subregional. Los Estados también han apuntado que es útil proporcionar creación de capacidad para que se puedan elaborar documentos nacionales de posición sobre la aplicabilidad del derecho internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados.

28. Entre los recursos en línea sobre creación de capacidad en el ámbito del derecho internacional disponibles a escala mundial cabe mencionar la guía sobre derecho cibernético elaborada por un consorcio integrado por el Organismo Nacional de Ciberseguridad y Seguridad de la Información de Chequia, el CICR, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, la Universidad de Exeter, United States Naval War College y la Universidad de Wuhan[12]. Esta guía, que los profesionales de los sectores público y jurídico tienen a su disposición de forma gratuita, consta de: a) 28 hipótesis en las que se explora la aplicabilidad del derecho internacional a las ciberoperaciones; b) información sobre las distintas posturas nacionales en cuanto a la aplicación del derecho internacional al uso de las tecnologías de la información y las comunicaciones, también en lo relativo a la soberanía, a la no intervención o a qué constituye un ataque en el marco del derecho

[10] Véase https://www.oas.org/ext/es/seguridad/prog-ciber.

[11] Véase https://dialogo-americas.com/es/articles/brasil-lidera-foro-iberoamericano-de-ciberdefensa/.

[12] Véase https://cyberlaw.ccdcoe.org/wiki/Main_Page.

internacional humanitario; y c) más de 50 páginas de ciberincidentes, en las que se recoge información sobre ataques recientes o sobre conflictos armados en curso.

29. En 2020 el Instituto de Ética, Derecho y Conflictos Armados de la Universidad de Oxford puso en marcha el Proceso de Oxford sobre las Protecciones del Derecho Internacional en el Ciberespacio en colaboración con Microsoft[13]. Hasta el momento de redactar el presente documento el Proceso de Oxford había elaborado cinco "declaraciones de Oxford sobre las protecciones del derecho internacional", que son resultado de la colaboración entre juristas internacionales de todo el mundo y tienen como objeto definir y aclarar las normas del derecho internacional aplicables a las ciberoperaciones en diversos contextos, por ejemplo en cuanto a las protecciones del sector de la atención de la salud, la salvaguardia de la investigación sobre vacunas, la protección frente a la injerencia electoral y la regulación de las operaciones y actividades informativas y de las operaciones de *ransomware*.

30. En lo relativo a la aplicabilidad del derecho internacional humanitario al ciberespacio, el CICR ofrece diversos recursos a las instancias normativas, tales como artículos de investigación, talleres y simposios, y además ha creado una delegación del CICR sobre el ciberespacio con sede en Luxemburgo, país del que también recibe apoyo. Como ejemplos de sus actividades más recientes cabe señalar la puesta en marcha de un programa de acción humanitaria en cooperación con el Centro de Investigación sobre Artes, Ciencias Sociales y Humanidades de la Universidad de Cambridge, la organización junto con la Academia de Derecho Internacional Humanitario y Derechos Humanos de Ginebra de una reunión internacional de expertos sobre derecho internacional humanitario y la creciente participación de civiles en ciberoperaciones y otras operaciones digitales durante conflictos armados, que tuvo lugar los días 28 y 29 de septiembre de 2023 en Ginebra, y la celebración, en alianza con Research Society of International Law, de una mesa redonda sobre ciberguerra el 17 de mayo en 2023 en Islamabad.

31. Australia, Países Bajos (Reino de los) y Singapur, en alianza con Cyber Law International, se han coordinado para impartir un curso dirigido a funcionarios de los Estados miembros de la ASEAN y la OSCE sobre ciberderecho internacional, en particular sobre el derecho internacional de las ciberoperaciones.

32. La Agencia de Cooperación Internacional del Japón organiza un curso sobre creación de capacidad en derecho internacional y formación de políticas para mejorar las medidas de ciberseguridad a fin de suministrar a los funcionarios de organismos públicos y equipos nacionales de respuesta a emergencias informáticas de países en desarrollo los conocimientos y las aptitudes que necesitan para elaborar y aplicar eficazmente políticas de ciberseguridad.

33. Los Estados también han llevado a cabo varias consultas para poder dialogar sobre la aplicabilidad del derecho internacional. Por ejemplo, la OEA ha organizado, en cooperación con el Comité Jurídico Interamericano y el CICR, consultas sobre el derecho internacional aplicable al ciberespacio[14]. Además, en colaboración con el Instituto de Derecho, Innovación y Tecnología de la Universidad Temple (Pennsylvania) y Microsoft, México organizó sendos talleres virtuales sobre la aplicación del derecho internacional al ciberespacio, la promoción de normas sobre el comportamiento pacífico, y el cierre de la brecha digital. Este proyecto culminó en un compendio multipartito de buenas prácticas y recomendaciones sobre la aplicación del derecho internacional al ciberespacio, que se presentó en el sexto período de sesiones sustantivo del grupo de trabajo de composición abierta sobre la seguridad de

[13] Véase https://www.elac.ox.ac.uk/the-oxford-process/.

[14] Véase https://www.oas.org/en/sla/dil/International_Law_Applicable_to_Cyberspace_2022.asp.

las tecnologías de la información y las comunicaciones y de su uso, en diciembre de 2023.

34. La OSCE ha organizado cursos ejecutivos sobre el derecho internacional de las ciberoperaciones, uno de los cuales se celebró del 13 al 17 de febrero de 2023 en Skopie en cooperación con el Reino de los Países Bajos y con el apoyo de Eslovaquia, Italia, el Reino Unido de Gran Bretaña e Irlanda del Norte, la República de Corea y Suiza y de Cyber Law International.

Políticas, incluida la formulación de estrategias nacionales

35. En el anexo B de su segundo informe anual (A/78/265), el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) recogió la lista inicial de medidas globales voluntarias de fomento de la confianza acordadas, una de las cuales es seguir compartiendo información de forma voluntaria, como documentos conceptuales y estrategias, políticas y programas nacionales. Además, los Estados han reconocido que es importante poseer la capacidad necesaria para instaurar las políticas, leyes y estrategias indispensables para lograr un entorno de las tecnologías de la información y las comunicaciones seguro. En este contexto se han llevado a cabo varios esfuerzos de creación de capacidad para ayudar a los Estados a formular políticas nacionales, elaborar estrategias y establecer las instituciones y estructuras necesarias con competencia en cuestiones relacionadas con las tecnologías de la información y las comunicaciones en el contexto de la seguridad nacional.

36. A escala mundial, el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) celebra todos los años una conferencia sobre ciberestabilidad en la que se debate sobre cómo promover un ciberespacio seguro y estable, sobre las normas y el derecho internacional y sobre cómo apoyar el diálogo multilateral en torno a cuestiones de ciberseguridad. En ediciones pasadas de la conferencia se celebraron sesiones informativas temáticas impartidas por académicos como apoyo para las opiniones nacionales de los Estados, por ejemplo sobre cuestiones jurídicas relacionadas con el arreglo pacífico de controversias en relación con el uso de las tecnologías de la información y las comunicaciones por parte de los Estados y sobre cuestiones normativas y técnicas concernientes a la protección de infraestructura y servicios críticos de diversos sectores. También se trataron los procesos intergubernamentales conexos en el marco de las Naciones Unidas. La próxima edición de la conferencia sobre ciberestabilidad tendrá lugar los días 29 de febrero y 1 de marzo de 2024 en Nueva York.

37. Los Estados también han reconocido el valor del Portal de Política Cibernética del UNIDIR, que presenta un formato útil para que los Estados actúen voluntariamente con transparencia y compartan información, políticas, leyes y buenas prácticas pertinentes[15]. Hasta diciembre de 2023 se habían subido a la base de datos del Portal 1.528 documentos, había datos en 55 idiomas y se había publicado información sobre 897 proyectos de creación de capacidad. En 2023 el Portal recibió aproximadamente 23.000 visitas.

38. En diciembre de 2023 el Portal de Política Cibernética pasó a incluir casi 900 proyectos de creación de capacidad del portal Cybil del Foro Mundial de Competencia Cibernética. Los datos transferidos de cada proyecto se refieren al título, los destinatarios, la instancia que los financia y las fechas de inicio y finalización, y se pueden consultar en los seis idiomas oficiales de las Naciones Unidas. Esta iniciativa mejora la seguridad de las tecnologías de la información y las comunicaciones y de su uso creando conciencia sobre los recursos disponibles, facilitando la colaboración

[15] Véase https://cyberpolicyportal.org/.

entre interesados y alentando una mayor transparencia en los esfuerzos de creación de cibercapacidad.

39. La UIT, en colaboración con el Banco Mundial, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) y la Organización de Telecomunicaciones del Commonwealth, presta apoyo relacionado con las políticas para crear un marco nacional de ciberseguridad eficaz. A tal efecto, la segunda edición de la guía para elaborar una estrategia nacional de ciberseguridad, publicada por la UIT en 2021[16], brinda a las instancias normativas una panorámica general del proceso de elaboración de la estrategia y prevé tener en cuenta también la situación concreta y los valores culturales y sociales de cada país. Además, la UIT ofrece un curso de capacitación en línea, integrado por cuatro módulos de aprendizaje electrónico y un ejercicio de simulación tomando como base la guía, para preparar a los responsables de formular políticas en cada país y los profesionales de la ciberseguridad de los sectores público y privado[17]. También existe en Internet un repositorio actualizado de estrategias nacionales de ciberseguridad en el que se pueden encontrar políticas, planes de acción y otros elementos pertinentes relacionados con la ciberseguridad[18].

40. En el marco del Programa de Becas sobre Ciberseguridad de las Naciones Unidas y Singapur se organizan cada año dos sesiones de seis días de duración para funcionarios públicos a fin de crear capacidad y redes sobre políticas, estrategias y operaciones nacionales en materia de ciberseguridad y seguridad digital. Se han celebrado ya tres ediciones del Programa, y hay dos sesiones previstas para 2024. Existe una red de exbecarios integrada por más de 70 personas procedentes de 62 Estados Miembros.

41. El Reino de los Países Bajos financió el ciclo Diálogo Global sobre Ciberpolíticas con la entidad Observer Research Foundation America. En el transcurso de más de dos años, el proyecto apoyó la elaboración de estrategias nacionales de ciberseguridad y organizó diálogos regionales sobre ciberpolíticas en Asia Sudoriental, los Balcanes Occidentales, Oriente Medio y Norte de África, África Meridional y América Latina y el Caribe. También trató de promover la transformación digital segura y alianzas público-privadas, de definir las necesidades y lagunas en materia de creación de capacidad y de respaldar que prosiguiera la elaboración de normas sobre el comportamiento de los Estados en el ciberespacio.

42. En el marco del Digital for Development Hub, la Unión Europea, Alemania, Expertise France, la Fundación Internacional para Iberoamérica de Administración y Políticas Públicas y la Iniciativa del Cuerno de África han colaborado en una iniciativa de gobierno digital y ciberseguridad para la región del Cuerno de África[19] cuyo fin es ayudar a los Estados participantes (Djibouti, Kenya y Somalia) a reforzar la prestación de servicios del sector público mediante canales digitales seguros. En el marco de este proyecto se celebran diálogos e intercambios de información en el seno de un comité técnico regional, y en cada Estado hay en marcha exámenes de hojas de ruta y proyectos de digitalización.

43. En la esfera bilateral, Francia y el Senegal colaboran en la escuela nacional de ciberseguridad, que tiene orientación regional y sede en Dakar y que, entre otras cosas, organiza cursos de capacitación, refuerza la cooperación y crea conciencia sobre la importancia de la ciberseguridad entre los Estados de África[20]. Como ejemplo

[16] Véase https://ncsguide.org/the-guide/.

[17] Véase https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

[18] Véase https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[19] Véase https://www.fiiapp.org/proyectos_fiiapp/initiative-d4d-para-el-gobierno-digital-y-la-ciberseguridad-idgc-para-la-iniciativa-del-cuerno-de-africa/.

[20] Véase https://www.diplomatie.gouv.fr/en/country-files/senegal/news/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal.

de país que tiene en marcha múltiples programas bilaterales cabe destacar a Portugal, que apoya programas de cooperación estratégica en alianza con Angola, Cabo Verde, Guinea-Bissau, Mozambique, Santo Tomé y Príncipe y Timor-Leste para fortalecer las estructuras jurídicas y administrativas a fin de prevenir y detectar delitos cibernéticos, actos de ciberterrorismo e incidentes cibernéticos y responder a ellos.

44. En Asia, el Centro Mundial de Ciberseguridad para el Desarrollo, con sede en la República de Corea, presta asistencia a los Estados que la solicitan para crear ciberexperiencia y ciberresiliencia en el sector público. Puede organizar seminarios sobre cómo elaborar estrategias y marcos nacionales de ciberseguridad, sobre cómo crear y gestionar equipos nacionales de respuesta a emergencias informáticas, sobre cómo detectar y analizar ciberincidentes y responder a ellos y sobre cómo compartir información relativa a tendencias y amenazas cibernéticas[21]. Recientemente se han organizado seminarios en Costa Rica, la República Democrática Popular Lao y Serbia sobre la elaboración de estrategias de seguridad, gestión de incidentes, ciberseguridad y resiliencia, entre otros temas.

45. En el marco de su Programa de Cooperación sobre Cibernética y Tecnología Crítica, el Departamento de Relaciones Exteriores y Comercio de Australia ayuda a su Comisionado de Seguridad Electrónica a elaborar recursos sobre seguridad en línea de alcance mundial y a trabajar con gobiernos de Asia y el Pacífico para formular enfoques nacionales a fin de proteger a la ciudadanía en línea[22]. En colaboración con la industria, el mundo académico, la sociedad civil, organismos del Gobierno de Australia y otros donantes con ideas afines, el Programa ayuda a más de 25 países de Asia Sudoriental y el Pacífico a promover y proteger sus intereses colectivos en el ciberespacio.

46. En América, en el marco de la Cumbre de Líderes de América del Norte, el Canadá, los Estados Unidos de América y México participaron en una mesa redonda sobre ciberseguridad para reforzar la cooperación entre los Estados participantes a la hora de elaborar y aplicar políticas de ciberseguridad, que tuvo lugar en enero de 2023. Del 8 al 14 de octubre de 2023, Chequia y Colombia organizaron debates sobre la intersección de la ciberseguridad y la inteligencia artificial centrados en la legislación, las políticas nacionales y las estrategias.

47. La Iniciativa sobre Ciberdiplomacia de la Unión Europea (Cyber Direct) respalda una amplia gama de esfuerzos de apoyo normativo, investigación, extensión y creación de capacidad en el ámbito de la ciberdiplomacia; por ejemplo, mantiene una guía sobre ciberdiplomacia y organiza todos los años el Diálogo Europeo sobre Ciberdiplomacia[23]. Entre otros muchos programas e iniciativas, Cyber Direct organiza un programa de becas para ciberexpertos y expertos digitales que estén comenzando su carrera profesional o que tengan algunos años de experiencia y procedan de países asociados, a saber, países que no sean miembros de la Unión Europea y pertenezcan al Grupo de Europa Oriental, al Grupo de África, al Grupo de América Latina y el Caribe o el Grupo de Asia y el Pacífico[24]. También en la misma región, una coalición integrada por Alemania, Estonia, Finlandia y Luxemburgo y dirigida por la Autoridad de Sistemas de Información de Estonia gestiona y ejecuta la iniciativa CyberNet (2019-2025) de la Unión Europea[25], que ha creado una comunidad de más de 300 ciberexpertos en más de 40 ámbitos de competencia para apoyar el desarrollo de la cibercapacidad.

[21] Véase https://www.kisa.or.kr/EN/201.
[22] Véase https://www.internationalcybertech.gov.au/cyber-tech-cooperation-program.
[23] Véase https://eucyberdirect.eu/.
[24] Véase https://eucyberdirect.eu/news/eu-cd-fellowship.
[25] Véase https://www.eucybernet.eu/.

48. El Centro de Ginebra para la Gobernanza del Sector de Seguridad gestiona un programa de gobernanza de la ciberseguridad que presta apoyo a actores estatales en materia de legislación y políticas sobre ciberseguridad a fin de reforzar los marcos de rendición de cuentas y crear capacidad[26]. En el marco de un proyecto reciente se creó la Red de Investigaciones sobre Ciberseguridad de los Balcanes Occidentales, que, entre otras actividades, investiga sobre ciberseguridad y derechos humanos, las necesidades de ciberseguridad de los grupos vulnerables y el género en los distintos contextos nacionales. El Centro de Ginebra para la Política de Seguridad organiza asimismo cursos de capacitación y talleres sobre ciberseguridad[27]. También con sede en Ginebra, DiploFoundation respalda el desarrollo de la capacidad en el ámbito de la gobernanza de Internet y las políticas digitales organizando simulacros, talleres y cursos en línea en materia de ciberseguridad, datos, inteligencia artificial y otras cuestiones incipientes y promoviendo y desarrollando herramientas digitales para que la gobernanza y la elaboración de políticas sean inclusivas y eficaces[28].

49. El proyecto Cyberspace4All, que cuenta con el apoyo del Reino de los Países Bajos, tiene como fin promover la inclusividad y la concienciación creando terminología y referencias comunes sobre la cibergobernanza internacional, informando sobre los principales acontecimientos relacionados con el mundo cibernético registrados en las Naciones Unidas y ayudando a fundamentar las políticas de los Estados sobre cibernormas. En su primera fase, el proyecto ha elaborado una edición de *Journal of Cyber Policy*, videos cortos sobre creación de cibercapacidad y un pódcast titulado *Who rules cyberspace?*. En la segunda fase, que se ejecuta conjuntamente con Chatham House, se pretende formular recomendaciones sobre las normas y los principios de las Naciones Unidas relativos a la creación de capacidad y el comportamiento responsable de los Estados en el ciberespacio, crear conciencia sobre dichas normas y principios y apoyar su aplicación.

50. Se han organizado esfuerzos de creación de capacidad en el ámbito de la ciberdiplomacia por varias vías. Un ejemplo es la Escuela de Verano de Ciberdiplomacia de Tallin, que forma parte del Programa de Multilateralismo y Digitalización y se organiza en cooperación con el Ministerio de Relaciones Exteriores de Estonia, la Academia de Gobernanza Electrónica y el Centro de Desarrollo Internacional de Estonia. Su principal objetivo es brindar formación a los diplomáticos que trabajan en ciberpolítica exterior, así como a otros funcionarios públicos interesados en ciberproblemas complejos. El Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la OEA organiza también un programa de capacitación sobre ciberdiplomacia para prestar apoyo a los funcionarios que trabajan en este ámbito. En lo que respecta a la Secretaría de las Naciones Unidas, el curso en línea sobre ciberdiplomacia disponible en el portal Disarmament Education Dashboard se actualizará en 2024[29].

Equipos de respuesta a emergencias informáticas, capacitación técnica y otro apoyo conexo

51. Los Estados han pedido sistemáticamente que se adopte un enfoque de la creación de capacidad concreto y orientado a la acción, y han concluido que tales medidas concretas podrían consistir en la prestación de apoyo a los equipos de respuesta a emergencias informáticas o los equipos de respuesta a incidentes de seguridad informática y la formulación de cursos especializados y planes de estudio adaptados, entre ellos programas de formación de formadores y certificaciones

[26] Véase https://www.dcaf.ch/cybersecurity-governance.
[27] Véase https://www.gcsp.ch/.
[28] Véase https://www.diplomacy.edu/.
[29] Véase https://cyberdiplomacy.disarmamenteducation.org/home/.

profesionales. Los Estados han expresado también su preocupación por el hecho de que la falta de concienciación sobre las amenazas actuales y potenciales y la falta de capacidades adecuadas para detectar las actividades malintencionadas en la esfera de las tecnologías de la información y las comunicaciones, defenderse contra ellas o responder a ellas puedan hacerlos más vulnerables.

52. Se ha destacado asimismo la importancia de impartir capacitación técnica al personal en la esfera de las tecnologías de la información y las comunicaciones, en particular sobre seguridad de la información, métodos de detectar y contrarrestar ataques contra redes de computadoras en sistemas de información abiertos, tácticas, técnicas y procedimientos para proteger la información de intentos de acceso no autorizados, recopilación de datos de código abierto, técnicas de investigación de delitos relacionados con las tecnologías de la información y las comunicaciones en lo tocante a la paz y la seguridad internacionales y la cooperación internacional en este ámbito, informática forense, lucha contra el uso de las tecnologías de la información y las comunicaciones y los servicios postales internacionales en el tráfico de drogas y para el robo de fondos, y detección e investigación de transacciones ilegales con activos digitales, como las criptomonedas, y de su uso para financiar el terrorismo.

53. A escala mundial, la UIT presta asistencia a los Estados para crear equipos de respuesta a emergencias informáticas[30]. A título ilustrativo, recientemente se han creado equipos con el apoyo de la UIT en las Bahamas, Barbados, Burkina Faso, Chipre, Gambia, Ghana, Côte d'Ivoire, Jamaica, Kenya, Kirguistán, el Líbano, Malawi, Montenegro, la República Unida de Tanzanía, Trinidad y Tabago, Uganda y Zambia. Todos estos equipos actúan como órgano coordinador central encargado de detectar y gestionar ciberamenazas y responder a ellas.

54. La entidad Forum of Incident Response and Security Teams mantiene una red de más de 700 equipos de respuesta a emergencias informáticas para fomentar la cooperación a fin de responder, tanto de manera proactiva como reactiva, a los incidentes de ciberseguridad. Entre otras actividades, comparte mejores prácticas entre sus miembros y promueve coloquios técnicos, clases, publicaciones, servicios web, grupos de interés especial y una conferencia anual sobre respuesta a incidentes[31].

55. En el marco de la presidencia de la India del Grupo de los 20, el Secretario del Ministro de Electrónica y Tecnología de la Información de la India, Alkesh Kumar Sharma, inauguró el simulacro sobre ciberseguridad del Grupo de los 20, en el que participaron más de 400 personas tanto de dicho país como de otros países. El Equipo de Respuesta a Emergencias Informáticas de la India organizó el simulacro en formato híbrido. A distancia asistieron participantes de unos 12 países. Los participantes de la India, pertenecientes a los sectores de las finanzas, la educación, las telecomunicaciones, la gestión portuaria y el transporte, la energía y las tecnologías de la información y las comunicaciones, asistieron tanto en persona como virtualmente.

56. En cuanto Presidencia en Ejercicio del Commonwealth, el Reino Unido llevó a cabo diversas actividades de creación de capacidad en el marco del Programa de Ciberseguridad del Commonwealth para apoyar los objetivos de la Ciberdeclaración del Commonwealth de 2018[32]. El Programa ayudó a los Estados miembros del Commonwealth a llevar a cabo autoevaluaciones de la capacidad nacional de ciberseguridad y prestó asistencia técnica, capacitación y asesoramiento sobre ciberseguridad y amenazas concernientes a delitos cibernéticos. En el marco del

[30] Véase https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx.
[31] Véase https://www.first.org/.
[32] Véase https://assets.publishing.service.gov.uk/media/60538ad98fa8f55d38ea34c3/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf.

proyecto se celebraron más de 140 eventos en 32 países y recibieron capacitación más de 6.000 personas.

57. El Centro de Excelencia de Ciberseguridad ASEAN-Singapur ofrece apoyo a los Estados miembros de la ASEAN para promover la creación de cibercapacidad en la región, en particular llevando a cabo investigaciones, impartiendo capacitación, prestando apoyo técnico relacionado con los equipos de respuesta a emergencias informáticas, facilitando el intercambio de información sobre ciberamenazas de código abierto, ataques y mejores prácticas conexas y organizando cursos de formación y simulacros[33]. Desde que se creó ha impartido más de 50 programas, a los que asistieron más de 1.600 altos funcionarios de los Estados participantes. A partir de 2024 también podrán participar en sus programas Estados de fuera de la región de la ASEAN. En aras de la coordinación y la cooperación, el Grupo de Trabajo sobre Ciberseguridad de la Reunión de Ministros de Defensa de la ASEAN Plus se viene reuniendo periódicamente desde 2016 como plataforma de fomento de la confianza y elaboración de normas entre los Estados miembros de la ASEAN.

58. El Programa de Cibercapacidad de la ASEAN tiene como finalidad crear capacidad en los Estados miembros de la ASEAN fortaleciendo la resiliencia y las respuestas de la región a las amenazas[34]. Entre las actividades organizadas en el marco del Programa cabe señalar talleres, seminarios, la Cibersemana Internacional de Singapur, de carácter anual, un taller sobre ciberseguridad conjunto de los Estados Unidos y Singapur y la Conferencia Ministerial de la ASEAN sobre Ciberseguridad. En la octava Cibersemana Internacional de Singapur, en 2023, se puso en marcha el Programa de Ciberliderazgo y Exalumnos de Singapur, que está abierto a candidatos de todos los Estados y organiza cursos básicos, ejecutivos y avanzados para funcionarios a fin de profundizar sus conocimientos sobre conceptos y procesos de ciberdiplomacia, derecho internacional, las normas en el ciberespacio y consideraciones operacionales y técnicas de ciberpolítica internacional. Se prevé crear además una beca de ciberliderazgo para exalumnos a fin de reunir a exparticipantes de las actividades de creación de capacidad organizadas por el Centro de Excelencia de Ciberseguridad en una serie de reuniones a puerta cerrada en torno a las tendencias y el discurso internacional sobre ciberseguridad, así como para intercambiar mejores prácticas en ámbitos como la fuerza de trabajo y el desarrollo de aptitudes, los marcos jurídicos y el cibercomportamiento responsable.

59. La República de Corea viene siendo la sede de la Alianza sobre Ciberseguridad para el Progreso Mutuo desde que se creó, en 2016. La Alianza se centra en promover la cooperación y la creación de capacidad entre los Estados participantes[35]. En el momento de redactar el presente documento formaban parte de la Alianza 67 organizaciones de 49 países.

60. En 2023 el Organismo de Internet y Seguridad de Corea puso en marcha, en cooperación con la Universidad Nacional Kangwon, la Universidad Gangneung Wonju y la Universidad Tecnológica de Brunei, el proyecto Cyber Shield de la ASEAN, cuyo fin es mejorar la cooperación entre los Estados miembros de la ASEAN en materia de ciberseguridad e implantará un plan de estudios en línea sobre ciberseguridad en la región, investigará sobre los sistemas de certificación en materia

[33] Véase https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence.

[34] Véase https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.

[35] Véase https://www.cybersec-alliance.org/camp/index.do.

de ciberseguridad y organizará hackatones de la ASEAN e intercambios de estudiantes de ciberseguridad[36].

61. Entre 2017 y 2019 la UIT llevó a cabo un proyecto para ayudar a los pequeños Estados insulares del Pacífico a crear marcos de ciberseguridad nacionales, subregionales y regionales y para desarrollar las aptitudes en este ámbito. En este programa se evaluó la preparación para crear equipos de respuesta a emergencias informáticas en Papua Nueva Guinea, Samoa, Tonga y Vanuatu, y se diseñaron y elaboraron planes de implementación para tales equipos. En el marco del proyecto la UIT organizó talleres de capacitación para crear conciencia y desarrollar aptitudes, y en ellos más de 200 personas y más de 70 organizaciones compartieron su experiencia en el ámbito de la respuesta a incidentes y la protección de la infraestructura crítica de información. Además, se hizo un análisis de la situación vigente y los resultados se compararon con los indicadores del Modelo de Madurez de Capacidades de Ciberseguridad para Naciones, elaborado por el Centro Mundial de Capacidad sobre Ciberseguridad de Oxford Martin School, perteneciente a la Universidad de Oxford[37].

62. La Red Operacional de Ciberseguridad del Pacífico, parte integrante del Programa de Cooperación sobre Cibernética y Tecnología Crítica de Australia, es una red integrada por profesionales de la ciberseguridad de la región del Pacífico[38]. Mantiene un registro de puntos de contacto operacionales sobre ciberseguridad y posibilita que los miembros intercambien información sobre amenazas en materia de ciberseguridad, brinda a los expertos técnicos la oportunidad de compartir herramientas, técnicas e ideas y facilita la cooperación y la colaboración, en particular cuando la región se ve afectada por un incidente de ciberseguridad.

63. Se han llevado a cabo asimismo varias actividades bilaterales centradas en las capacidades técnicas. Por ejemplo, en Nueva Zelandia, el Programa de Creación de Capacidad sobre Ciberseguridad en el Pacífico presta apoyo bilateral a los Estados insulares del Pacífico para elaborar estrategias nacionales de ciberseguridad, desarrollar las capacidades de los equipos de respuesta a emergencias informáticas, crear conciencia, redactar legislación sobre ciberseguridad y ciberdelincuencia de acuerdo con las normas internacionales e investigar y enjuiciar delitos cibernéticos de conformidad con dicha legislación. Recientemente se han celebrado en la región diversas conferencias, como el Simposio Internacional sobre Respuesta a los Delitos Cibernéticos, que tuvo lugar en la República de Corea del 13 al 15 de septiembre de 2023, y la Conferencia de Cooperación y Creación de Cibercapacidad en el Pacífico, que tuvo lugar en Fiji del 2 al 4 de octubre de 2023.

64. Por conducto de su Programa de Cooperación sobre Cibernética y Tecnología Crítica, Australia ayuda a asociados del Pacífico y de Asia Sudoriental a reforzar su resiliencia técnica y de gobernanza ante las ciberamenazas[39]. El Programa se creó en 2016 y en 2021 se amplió para incluir la cooperación en cuanto a tecnologías críticas. Hasta noviembre de 2023 había respaldado 126 proyectos en 21 países de la región. Entre los proyectos se cuentan actividades para mejorar las capacidades relacionadas con la ciberseguridad, aprovechar la tecnología en apoyo del crecimiento económico y el desarrollo, abogar por la protección de los derechos humanos y la democracia en línea, evitar y enjuiciar los delitos cibernéticos y promover la aplicación del marco normativo respaldado por las Naciones Unidas sobre el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. El Proyecto de Cibercapacitación Intensiva, que se puso en marcha en agosto de 2019 en el marco del Programa de Cooperación,

[36] Véase https://wwwk.kangwon.ac.kr/english/contents.do?key=2356&.
[37] Véase https://gcscc.ox.ac.uk/the-cmm.
[38] Véase https://pacson.org/.
[39] Véase https://www.internationalcybertech.gov.au/our-work/capacity-building.

tenía como finalidad brindar formación especializada práctica a funcionarios públicos de Asia Meridional sobre desafíos y oportunidades comunes.

65. El Centro de Cibercapacidades de Latinomérica y el Caribe, que se creó en 2022, recibe el apoyo de la Unión Europea y tiene su sede en la República Dominicana, imparte formación y creación de capacidad a los Estados de América Latina y el Caribe para abordar la ciberseguridad y la ciberdelincuencia. Entre las actividades que lleva a cabo se cuentan el suministro de material de formación y la organización de cursos, la creación de conciencia y la provisión de apoyo a las instancias normativas sobre la transformación digital y de la ciberseguridad en el plano nacional y sobre consultas nacionales y regionales en torno a cuestiones relacionadas con la ciberseguridad. También se han puesto en marcha esfuerzos bilaterales para ayudar a crear equipos nacionales de respuesta a emergencias informáticas, entre ellos un proyecto de la Agencia Brasileña de Cooperación para ayudar a crear un centro de respuesta a incidentes de ciberseguridad en Suriname.

66. Entre 2016 y 2019 el Programa Mundial de Capacidad sobre Ciberseguridad, financiado por el Mecanismo de la Alianza de la República de Corea y el Banco Mundial, proporcionó asistencia técnica nacional y regional adaptada a un grupo de seis países de distintas regiones[40]. Cada Estado participante se sometió a una evaluación tomando como referencia el Modelo de Madurez de Capacidades de Ciberseguridad para Naciones, sobre la base de la cual se proporcionaron informes analíticos, capacitación, talleres y asistencia técnica. El proyecto tenía como finalidad ayudar a los Estados participantes a reforzar el entorno nacional de ciberseguridad y contó con la participación de las instancias responsables de elaborar políticas de ciberseguridad y los interesados pertinentes. La eficacia de las intervenciones se cuantificó mediante evaluaciones del impacto.

Otros ámbitos de creación de capacidad

67. Se están llevando a cabo asimismo esfuerzos de creación de capacidad en otras esferas transversales y temáticas, entre otras cosas centrados en grupos específicos, como las mujeres, la juventud, el mundo académico y la industria. Otros ámbitos de atención son la concienciación del público, el acceso y la alfabetización digitales y la lucha contra los delitos cibernéticos.

Género y participación de las mujeres

68. La Beca Mujeres y Seguridad Internacional y Ciberespacio es una iniciativa conjunta de Australia, el Canadá, los Estados Unidos, Nueva Zelandia, Países Bajos (Reino de los) y el Reino Unido que se puso en marcha en 2020[41]. Facilita la asistencia de diplomáticas a las reuniones de los procesos intergubernamentales conexos que se celebran bajo los auspicios de las Naciones Unidas, incluido el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, y organiza talleres y cursos de formación práctica sobre negociación. En su segunda edición, el programa presta apoyo a 35 diplomáticas procedentes de diversos países de la ASEAN, Asia y el Pacífico, Sudamérica y el Commonwealth para que participen en las reuniones del grupo de trabajo. Las becarias también reciben capacitación del Instituto de las Naciones Unidas para Formación Profesional e Investigaciones sobre negociaciones multilaterales, participan en una sesión de introducción a cuestiones pertinentes para la seguridad

[40] Véase https://www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp.

[41] Véase https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship.

internacional en el ciberespacio y reciben asesoramiento de colegas con más experiencia que trabajan en estas cuestiones en las Naciones Unidas en Nueva York.

69. La UIT gestiona en la actualidad un programa titulado Her Cybertracks que promueve la representación equitativa, plena y significativa de las mujeres en el ámbito de la ciberseguridad[42]. El programa ayuda a las participantes a desarrollar sus aptitudes para implicarse en la formulación de políticas sobre ciberseguridad a escala nacional e internacional y trata de concienciar y reducir los obstáculos a la participación de las mujeres en este campo y aumentar la participación y la representación de las mujeres en la fuerza de trabajo en materia de ciberseguridad. En Asia Sudoriental, la UIT ha ejecutado un proyecto para mejorar la elaboración de normas y marcos sobre tecnologías críticas que fomenten la implicación, la inclusión y el empoderamiento de las mujeres. Este proyecto apoya la elaboración de políticas, normas, marcos e iniciativas para mitigar el sesgo y fomentar la confianza y la inclusión. Inicialmente se implementó en Filipinas, Indonesia, Malasia y Tailandia, pero está previsto ampliarlo a otros Estados de la región.

70. La UIT también ofrece un Programa de Mentorías para Mujeres sobre Cibernética. La primera edición se puso en marcha en 2021, coincidiendo con el Día Internacional de la Mujer, y fue organizada conjuntamente por la UIT, la entidad Forum of Incident Response and Security Teams e “Iguales”, la Alianza Mundial para la Igualdad de Género en la Era Digital. Desde que dio comienzo han recibido capacitación y mentoría casi 300 mujeres de 73 países.

Implicación de la juventud y concienciación

71. A los efectos de crear conciencia entre la juventud interesada en seguridad de las tecnologías de la información y las comunicaciones, implicarla y desarrollar su capacidad, el equipo de respuesta a emergencias informáticas de Türkiye organizó el concurso de ciberseguridad online Cyber Star, que duró 24 horas y siguió el formato de captura de bandera. En la edición de 2019 compitieron más de 20.000 participantes, tanto en equipo como a título individual. El equipo de respuesta a emergencias informáticas también gestiona el ciberprograma FETİH, cuyo fin es desarrollar las aptitudes de los participantes con miras a que entren en el sector.

72. Algunos Estados han hecho esfuerzos a escala nacional para crear conciencia sobre la importancia de las buenas prácticas en el ámbito de la ciberseguridad. Por ejemplo, en el mes de octubre la Guardia Nacional de México promueve actividades en el marco de la Semana Nacional de la Ciberseguridad, cuyo fin es reunir a representantes de todos los sectores pertinentes para intercambiar buenas prácticas y experiencias respecto de la protección de infraestructuras críticas, la seguridad de la ciudadanía en el ciberespacio, la economía digital, la privacidad y la armonización de los marcos legislativos nacionales.

[42] Véase https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx.

Colaboración con la industria y el sector privado

73. Diversos Estados han recalcado la utilidad de las alianzas público-privadas y de la colaboración con asociados de la industria para fomentar la ciberresiliencia. También han mencionado esfuerzos para llevar a cabo consultas con las principales organizaciones públicas y privadas a fin de evaluar el grado general de ciberseguridad nacional. En octubre de 2023 la Conferencia de Ciberseguridad de Kubán reunió a representantes de instituciones de educación superior, autoridades estatales y municipales y jefaturas de empresas e instalaciones de infraestructura de la Federación de Rusia y a miembros de la comunidad internacional para discutir los retos, las tareas y las tendencias actuales. En este evento también se organizó un concurso dirigido a la juventud denominado KubanCTF-2023[43].

74. A partir de las lecciones aprendidas y las mejores prácticas derivadas de la creación de soluciones en la nube y de seguridad a escala mundial para gobiernos y usuarios particulares, Google ha elaborado una hoja de ruta sobre ciberseguridad para que la examinen los Estados, cuyo fin es ayudarlos a elaborar estrategias nacionales de ciberseguridad para proteger la infraestructura crítica, la ciudadanía y la prosperidad económica[44].

Recursos y estudios de instituciones académicas

75. El Programa de La Haya sobre Ciberseguridad Internacional investiga sobre novedades digitales y cibernormas, organiza una conferencia académica anual y prepara una recopilación de las investigaciones y los debates académicos conexos[45]. Las publicaciones más recientes versaron sobre temas como la implicación de múltiples interesados en los procesos de elaboración de normas sobre ciberseguridad y el comportamiento responsable en el ciberespacio.

76. El Modelo de Madurez de Capacidades de Ciberseguridad para Naciones define cinco dimensiones de madurez en ciberseguridad y los pasos necesarios para alcanzarlas. Se ha implantado más de 130 veces en más de 90 Estados desde 2015, con el apoyo del Centro Mundial de Capacidad sobre Ciberseguridad y la cooperación de organizaciones internacionales y regionales y otras organizaciones asociadas. Con miras al futuro, el Centro está formulando una métrica adicional para el Modelo que cuantificará las capacidades relacionadas con la inteligencia artificial, a fin de ayudar a los Estados a adaptarse a ella y emplearla de manera segura y sostenible.

Desarrollo, acceso y alfabetización digitales

77. El Programa de las Naciones Unidas para el Desarrollo (PNUD) lleva a cabo varias iniciativas para fomentar la infraestructura digital, promover la alfabetización digital e implantar soluciones de gobernanza electrónica[46]. Por ejemplo, ha comenzado a utilizar la evaluación de la preparación digital para definir las intervenciones digitales más apropiadas y establecer prioridades entre ellas en el marco del plan de transformación digital de cada país. Esta evaluación se centra en el contexto digital del país en cuestión, que puede ser desde un contexto en el que no existan los fundamentos digitales básicos, o sí existan pero estén incompletos, hasta un contexto en el que lo digital sea el pilar del crecimiento y el desarrollo nacionales; estas distintas situaciones se conocen como etapas de preparación digital.

[43] Véase https://kubcsc.ru/en#events.
[44] Véase https://safety.google/intl/en_uk/.
[45] Véase https://www.thehagueprogram.nl/.
[46] Véase https://www.undp.org/digital.

78. El Programa de Acceso Digital del Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte trata de catalizar un acceso digital más inclusivo, asequible y seguro para comunidades del Brasil, Indonesia, Kenya, Nigeria y Sudáfrica[47].

79. La Iniciativa de Gobierno Digital y Ciberseguridad en los Países del Cuerno de África ayuda a los Gobiernos de Djibouti, Kenya y Somalia a reforzar la gobernanza electrónica y desarrollar servicios electrónicos centrados en las personas. En julio de 2023, en colaboración con Smart Africa por conducto de la entidad Smart Africa Digital Academy, Burkina Faso organizó cursos de certificación sobre computación en la nube y ciberseguridad.

80. La iniciativa Cyber4Good de la UIT tiene por objeto facilitar el acceso a los servicios y las herramientas digitales en los países menos adelantados, con la participación de actores del sector privado y el apoyo de la República de Corea[48]. En el marco del proyecto se creará un fondo de la UIT para el desarrollo de la ciberseguridad, que se regirá por un modelo de gobernanza y estará dirigido por una junta consultiva. El programa Ciberresiliencia para el Desarrollo de la Unión Europea ayuda a actores públicos y privados a reforzar la ciberseguridad y la resiliencia a escala mundial[49].

81. La Alianza del Banco Mundial para el Desarrollo Digital apoya la transformación digital inclusiva en más de 80 países[50]. El fondo fiduciario de donantes múltiples sobre ciberseguridad, que entró en funcionamiento en 2021 y recibe el apoyo de Alemania, Estonia, el Japón y Países Bajos (Reino de los), promueve el programa de desarrollo digital mediante investigaciones, apoyo programático y evaluación y mitigación de riesgos en la infraestructura crítica y en sectores de alto riesgo. En cooperación con la Unión Africana, la iniciativa Economía Digital para África del Banco Mundial respalda la aplicación de la Estrategia de Transformación Digital de la Unión Africana para 2020-2030, que, apoyándose en diversos pilares, como la infraestructura digital, los servicios, las aptitudes, un entorno normativo y regulatorio propicio e innovación y emprendimiento, define la ciberseguridad, la privacidad y la protección de los datos personales como tema transversal. Recoge propuestas detalladas para crear capacidad en materia de desarrollo, acceso y alfabetización digitales, incluido el fomento de la capacidad humana e institucional mediante campañas de concienciación, la capacitación profesional, la investigación y el desarrollo y los equipos de respuesta a emergencias informáticas[51].

Lucha contra los delitos cibernéticos

82. En 2013 se creó el Programa Mundial contra el Delito Cibernético, de la Oficina de las Naciones Unidas contra la Droga y el Delito. Su mandato figura en la resolución 65/230 de la Asamblea General y en las resoluciones 22/7 y 22/8 de la Comisión de Prevención del Delito y Justicia Penal, y, si bien se viene ejecutando sobre la base de dichas resoluciones, cabe señalar que en la actualidad la Asamblea General está negociando un tratado. Aborda los siguientes aspectos interrelacionados de la lucha contra los delitos cibernéticos: la prevención, la detección, la investigación, el enjuiciamiento y la imposición de penas o la decisión judicial.

83. La Organización Internacional de Policía Criminal (INTERPOL), por conducto de su Centro de Intercambio de Información sobre la Ciberdelincuencia, encabeza en

[47] Véase https://www.oecd.org/development-cooperation-learning/practices/leaving-no-one-behind-in-a-digital-world-the-united-kingdom-s-digital-access-programme-e8b15982/.
[48] Véase https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=2GLO21119.
[49] Véase https://cyber4dev.eu/.
[50] Véase https://www.digitaldevelopmentpartnership.org/.
[51] Véase https://www.worldbank.org/en/programs/all-africa-digital-transformation.

la actualidad el diseño y la prestación de asistencia técnica y capacitación específicas para las fuerzas del orden en relación con las tecnologías de la información y las comunicaciones y los delitos cibernéticos. El Centro ayuda a los países miembros a detectar ciberamenazas, elaborar estrategias de prevención y disrupción y coordinar su respuesta a tales amenazas.

Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines terroristas

84. El Programa Mundial Antiterrorismo sobre Ciberseguridad y Nuevas Tecnologías ayuda a los Estados Miembros y las organizaciones internacionales y regionales a diseñar y ejecutar respuestas eficaces a los retos y las oportunidades que dimanan de las tecnologías de la información y las comunicaciones en la lucha contra el terrorismo. Tiene como finalidad generar conocimiento y crear conciencia, así como mejorar las aptitudes y las capacidades necesarias para implementar respuestas normativas, proteger la infraestructura crítica frente a actos terroristas que utilicen las tecnologías de la información y las comunicaciones y potenciar las capacidades de justicia penal. En el marco del Programa han recibido capacitación más de 4.000 funcionarios de 150 Estados Miembros, se han organizado más de 60 talleres de capacitación y se han publicado 12 productos del conocimiento. También se ha prestado asistencia para la creación de capacidad sobre ciberseguridad, en particular organizando simulacros antiterroristas y otros ejercicios de simulación.

V. Observaciones y conclusiones de la Secretaría

85. La creación de capacidad en el ámbito de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional sigue siendo, acertadamente, una de las máximas prioridades de los Estados. Además, es en gran medida la base de los esfuerzos emprendidos respecto de todas las cuestiones relacionadas que aborda el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), a saber, las amenazas existentes e incipientes, la aplicabilidad del derecho internacional al uso de tales tecnologías por parte de los Estados y las medidas de fomento de la confianza. Muchos Estados también han destacado que es importante tratar la creación de capacidad en todo diálogo institucional periódico que se celebre bajo los auspicios de las Naciones Unidas en materia de seguridad de las tecnologías de la información y las comunicaciones. **En este sentido, la creación de capacidad debe seguir siendo un pilar fundamental y transversal de todos los debates conexos que mantengan los Estados en las Naciones Unidas sobre la seguridad de las tecnologías de la información y las comunicaciones. Para poder avanzar en todas las esferas conexas, desde las normas hasta el derecho internacional, pasando por las medidas de fomento de la confianza, hará falta dedicar recursos específicamente a aplicar las correspondientes medidas de creación de capacidad.**

86. El Secretario General ha subrayado que es crucial invertir en la alfabetización y la infraestructura digitales para cerrar la brecha digital (A/75/982). De igual modo, los Estados han insistido en que no todo el mundo disfruta por igual de los beneficios de la tecnología digital y, en consecuencia, han subrayado la necesidad de prestar la debida atención a la creciente brecha digital en el contexto de la aceleración de la implementación de los Objetivos de Desarrollo Sostenible, respetando al mismo tiempo las necesidades y prioridades nacionales de los Estados. **Por tanto, es esencial que la creación de capacidad en la esfera de las tecnologías de la información y las comunicaciones atienda las necesidades y prioridades de todos los Estados, en particular los países en desarrollo, con miras a cerrar la brecha digital,**

incluida la brecha digital de género. Los esfuerzos de creación de capacidad deben ser también un factor facilitador del desarrollo sostenible.

87. Por el momento se desconocen todos los efectos que tiene el rápido avance de la ciencia y la tecnología en la paz y la seguridad internacionales. Se prevé que las oportunidades y los riesgos derivados del rápido desarrollo de tecnologías emergentes, como la inteligencia artificial y las tecnologías cuánticas, tengan profundas repercusiones en las necesidades y las prioridades de los Estados en materia de creación de capacidad en las esferas técnica y normativa. Por un lado, para poder utilizar competencias relacionadas con las tecnologías de la información y las comunicaciones, por ejemplo para mejorar de la detección y el análisis de amenazas, responder de manera automatizada a incidentes y perfeccionar las herramientas de detección de malware y de detección y prevención de fraudes, es necesario aumentar la capacidad. Por otro, los esfuerzos de creación de capacidad son cruciales para que los Estados tengan las aptitudes y los conocimientos necesarios para afrontar desafíos como las actividades de tecnología de la información y las comunicaciones maliciosas basadas en la inteligencia artificial, el sesgo y la discriminación que son inherentes a los sistemas de inteligencia artificial, y cuestiones relacionadas con la transparencia. **Las iniciativas concretas de creación de capacidad podrían centrarse en la alfabetización y el aumento de los conocimientos sobre los efectos de estas tecnologías incipientes, la elaboración de estrategias nacionales sobre el diseño, el desarrollo y el uso responsables de las tecnologías incipientes, y los mecanismos de cooperación internacional para aumentar la ciberresiliencia mediante la transferencia de conocimientos, mejores prácticas y lecciones aprendidas.**

88. Uno de los desafíos para lograr que los esfuerzos de creación de capacidad sean eficaces y sostenibles sigue siendo el riesgo de duplicación. En este contexto cabe señalar que en la decisión 630 del Consejo de la Unión Internacional de Telecomunicaciones, aprobada en agosto de 2023, se encargó a la UIT que elaborara un recurso para los Estados Miembros que incluyera, entre otras cosas, información sobre los programas de creación de capacidad que implementa, así como otros programas pertinentes[52]. En la decisión se pidió además que el recurso se actualice para tener en cuenta los nuevos retos y las novedades. Los Estados han planteado periódicamente la cuestión de aprovechar las sinergias y las iniciativas existentes en este sentido. **A la luz del carácter universal del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, se alienta a los Estados a que utilicen este proceso intergubernamental para seguir definiendo cómo evitar la duplicación a fin de adecuar en la mejor medida posible las necesidades a los recursos.**

[52] Se puede consultar en https://www.itu.int/md/S23-CL-C-0124/es.