Naciones Unidas A/77/92

Asamblea General

Distr. general
8 de junio de 2022
Español
Original: árabe/español/inglés/
ruso

77º período de sesiones
Tema 94 de la lista preliminar*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y promoción del comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones

Informe del Secretario General

Índice

		Página
I.	Introducción	2
II.	Respuestas recibidas de los Gobiernos	2
	Armenia	2
	Australia	4
	Azerbaiyán	7
	Cuba	8
	Dinamarca	9
	Egipto	15
	Federación de Rusia	17
	Singapur	19
	Türkiye	23
	Ucrania	29
III.	Respuestas recibidas de organizaciones intergubernamentales	31
	Unión Europea	31

* A/77/50.

Se ruega reciclar

I. Introducción

1. El 6 de diciembre de 2021, la Asamblea General aprobó la resolución 76/19, titulada “Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y la promoción de un comportamiento responsable de los Estados en la utilización de las tecnologías de la información y las comunicaciones”, en relación con el tema 95 del programa, relativo a los “avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”.

2. En el párrafo 6 de la resolución 76/19, la Asamblea invitó a todos los Estados Miembros, teniendo en cuenta las evaluaciones y recomendaciones que figuraban en el informe 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 y en los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, a seguir comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

a) Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito;

b) El contenido de los conceptos mencionados en el informe del Grupo de Trabajo de Composición Abierta y los informes del Grupo de Expertos Gubernamentales.

3. En cumplimiento de esa solicitud, el 24 de enero de 2022 se envió una nota verbal a todos los Estados Miembros para invitarlos a proporcionar información sobre el tema.

4. Las respuestas recibidas hasta el momento en que se preparó el informe figuran en las secciones II y III. Las respuestas que se reciban después del 31 de mayo de 2022 se publicarán en el sitio web de la Oficina de Asuntos de Desarme (https://www.un.org/disarmament/ict-security) en el idioma original en que se hayan recibido.

II. Respuestas recibidas de los Gobiernos

Armenia

[Original: inglés]
[31 de mayo de 2022]

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional

El Gobierno de Armenia ha creado un consejo de digitalización para impulsar el desarrollo de las competencias digitales y la digitalización del sistema de administración pública y la economía. Según los datos de 2021, se han analizado cerca de 25 programas y documentos estratégicos y se está trabajando continuamente en los ámbitos de la identificación digital, la autenticación de documentos oficiales, las licencias electrónicas, la introducción de notificaciones individuales y públicas, y la introducción de sistemas unificados de justicia electrónica, así como en otra serie de cuestiones de la agenda digital.

La República de Armenia aprobó una estrategia de digitalización el 11 de febrero de 2021. La estrategia prevé la transformación digital del Gobierno, la

economía y la sociedad mediante la introducción y el desarrollo de tecnologías innovadoras, la ciberseguridad, la política de datos, los servicios electrónicos y los sistemas de administración electrónica, la coordinación de los procesos de digitalización, la definición de normas comunes y un entorno digital, así como las iniciativas que promuevan el uso de las tecnologías digitales en el sector privado de la economía y el desarrollo y la aplicación de programas que fomenten el uso de las herramientas electrónicas por parte de los ciudadanos.

En el marco de la estrategia de digitalización de Armenia para el periodo 2021-2025, está previsto llevar a cabo las siguientes iniciativas:

a) Llevar a cabo modificaciones legislativas y normativas-legales en el ámbito de la seguridad de la información;

b) Elaborar un concepto de política pública de datos abiertos;

c) Implantar la formación en ciberseguridad para los residentes de los pueblos fronterizos (actualmente, los cursos de ciberseguridad se imparten a los empleados del Estado);

d) Crear un centro nacional de ciberseguridad. En particular, se está estudiando la posibilidad de introducir criterios de ciberseguridad, la creación de grupos estatales de respuesta rápida y la puesta en marcha de actividades de concienciación pública destinadas a aumentar la ciberalfabetización.

El Ministerio de Industria de Alta Tecnología tiene previsto elaborar una política y un plan de acción globales para superar los retos en el ámbito de la ciberseguridad, que incluirá el proceso de creación del centro de ciberseguridad y la formación de mecanismos de gestión de riesgos y de respuesta rápida durante los desastres naturales, las emergencias y la ley marcial.

El Ministerio subraya la importancia de una estrecha colaboración con el sector privado, la cooperación interinstitucional, la localización de la experiencia internacional y la observación de las normas internacionales de ciberseguridad, la cooperación interestatal y la pertenencia a las estructuras internacionales de seguridad.

Armenia está desarrollando políticas y capacidades en el ámbito de la ciberseguridad con organizaciones internacionales y regionales, incluso mediante la participación de las instituciones armenias pertinentes en diversos seminarios temáticos, conferencias y formación.

La República de Armenia es parte del Convenio sobre la Ciberdelincuencia. Más recientemente, Armenia ha iniciado un procedimiento nacional para la firma del Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas.

Armenia está activamente involucrada en los esfuerzos 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. El Grupo de Trabajo tiene como objetivo único sentar las bases de las nuevas normas en el ámbito de las tecnologías de la información y la comunicación (TIC).

La cooperación en curso en el marco del proyecto CyberEast del Consejo de Europa tiene por objeto capacitar a los expertos de las instituciones gubernamentales armenias para contrarrestar las amenazas de la ciberdelincuencia.

Armenia también valora los continuos esfuerzos que se están llevando a cabo en el marco de las medidas de fomento de la confianza de la Organización para la

Seguridad y la Cooperación en Europa en el ámbito de las TIC, que contribuyen a crear transparencia, previsibilidad y estabilidad en dicho ámbito.

Al mismo tiempo, cabe destacar la cooperación con empresas supranacionales. Armenia acoge a empresas líderes en tecnologías de la información, como Synopsys, Mentor Graphics, National Instruments, Microsoft, VMware, D-Link, Oracle y Cisco, entre otras. Microsoft y Cisco colaboran regularmente o asisten a foros para apoyar al Gobierno de Armenia con los últimos avances en materia de ciberseguridad y defensa.

Australia

[Original: inglés]
[31 de mayo de 2022]

Australia acoge con beneplácito la oportunidad, en respuesta a la invitación formulada en la resolución 76/19 de la Asamblea General, de exponer al Secretario General sus opiniones sobre la promoción de un comportamiento responsable de los Estados en el ciberespacio. Esta presentación se basa en la información proporcionada por Australia en respuesta a anteriores resoluciones de la Asamblea General, incluida la más reciente de mayo de 2021 (véase A/76/187)[1]. Australia alienta a todos los Estados a que participen de forma proactiva en el suministro de actualizaciones periódicas al Secretario General, con el fin de aumentar la transparencia y fomentar la comprensión de los esfuerzos de los demás para promover el comportamiento responsable de los Estados en el ciberespacio.

Marco del comportamiento responsable de los Estados en el ciberespacio

En los informes de 2010, 2013 y 2015 del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional se afirma de manera acumulativa que el derecho internacional vigente es aplicable y esencial para mantener la paz y la estabilidad en el ciberespacio[2]. En los informes también se articulan 11 normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados, al tiempo que se reconoce la necesidad de adoptar medidas de fomento de la confianza y de coordinar la creación de capacidad. Combinados, estos cuatro principios se denominan a menudo el marco del comportamiento responsable del Estado en el ciberespacio.

Australia se congratula de que el informe de marzo de 2021 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 (A/75/816), negociado y aprobado por los 193 Estados Miembros de las Naciones Unidas, demuestre el compromiso universal con el marco. Además, Australia tuvo la satisfacción de contar con la participación de un destacado experto en el sexto Grupo de Expertos Gubernamentales sobre el Fomento del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, que proporcionó más orientaciones prácticas sobre cómo aplicar el marco (véase A/76/135), que posteriormente fue acogido con satisfacción por la Asamblea General en su resolución 76/19.

Australia reafirma su compromiso de actuar de conformidad con los informes acumulativos del Grupo de Expertos Gubernamentales y del Grupo de Trabajo. Australia sigue participando activamente en el grupo de trabajo de composición

[1] Resoluciones 65/41, 68/243, 70/237, 74/28 y 75/32.
[2] A/65/201, A/68/98 y A/70/174, respectivamente.

abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y su uso en el período 2021-2025, creado en virtud de la resolución 75/240, y es un copatrocinador comprometido de la propuesta de Francia y Egipto para el establecimiento de un programa de acción. Australia apoya el establecimiento de un programa de acción que proporcione un foro permanente, inclusivo y transparente para el debate en curso y la acción práctica sobre cuestiones cibernéticas bajo los auspicios de las Naciones Unidas.

En aras de la transparencia, Australia publicará en breve una actualización sobre cómo aplica y observa las 11 normas voluntarias y no vinculantes de comportamiento estatal responsable. Aunque las normas no sustituyen ni alteran las obligaciones o los derechos de los Estados en virtud del derecho internacional (que son vinculantes), Australia reafirma las 11 normas como un complemento del derecho internacional, que proporciona una orientación específica adicional sobre lo que constituye un comportamiento responsable del Estado en el uso de las tecnologías de la información y las comunicaciones. Australia también pondrá a disposición del público su autoevaluación inicial de nuestra aplicación de los cibercompromisos de las Naciones Unidas utilizando la encuesta nacional del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) a través del Portal de Ciberpolítica del Instituto en un futuro próximo. Australia recomienda a todos los Estados la realización de la encuesta nacional y les anima a considerar la posibilidad de hacer públicas sus autoevaluaciones. El estudio de la aplicación de las recomendaciones de las Naciones Unidas ofrece varias ventajas. En concreto, los Estados pueden identificar cómo han aplicado el marco, dónde pueden existir lagunas en la aplicación y cualquier obstáculo a la misma. Esto, a su vez, puede ayudar a desarrollar programas específicos de cooperación y desarrollo de capacidades, que podrían ser apropiados para superar cualquier brecha en la capacidad y/o las barreras a la implementación identificadas.

Derecho internacional

Australia anima a todos los Estados a seguir estudiando y a ser transparentes en cuanto a sus posiciones sobre cómo se aplica el derecho internacional al comportamiento de los Estados en el ciberespacio. Reiteramos que, incluso cuando los puntos de vista difieren, el desarrollo de la comprensión de las posiciones de los demás sobre cómo se aplica el derecho internacional en el ciberespacio aumenta la previsibilidad y reduce el riesgo de error de cálculo, que puede conducir a una escalada en la conducta de los Estados. Australia reitera además que el derecho internacional es más eficaz cuando los Estados aplican y cumplen sus obligaciones jurídicas internacionales y, cuando es necesario, cooperan para defender el derecho internacional y garantizar la responsabilidad por las violaciones.

Australia acogió con satisfacción las conclusiones contenidas en el informe 2021 del Grupo de Expertos Gubernamentales (A/76/135), según las cuales el derecho internacional humanitario se aplica a las ciberactividades en situaciones de conflicto armado.

La posición de Australia sobre cómo se aplica el derecho internacional a la conducta del Estado en el ciberespacio se presenta en una serie de documentos:

- La presentación 2021 de Australia contenida en el compendio oficial de contribuciones nacionales voluntarias sobre el tema de cómo se aplica el derecho internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados, presentada por los expertos gubernamentales participantes en el Grupo de Expertos Gubernamentales (A/76/136);

- estrategia de compromiso internacional de 2021 en materia de cibernética y tecnologías críticas;
- estudios de casos de 2020 sobre la aplicación del derecho internacional en el ciberespacio (presentado al grupo de trabajo de composición abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional);
- Suplemento de Derecho Internacional 2019;
- estrategia de cibergestión internacional 2017.

Además de la participación de Australia en los procesos de las Naciones Unidas sobre cómo se aplica el derecho internacional en el ciberespacio, Australia también se esfuerza por participar en estos debates en los foros regionales. A este respecto, Australia hizo una declaración en la quincuagésima novena sesión de la Organización Jurídica Consultiva Asiático-Africana sobre el derecho internacional en el ciberespacio a finales de 2021.

Disuasión y respuestas al comportamiento irresponsable del Estado

Australia no tolera las actividades en el ciberespacio que vayan en detrimento de la paz y la estabilidad internacionales o que sean contrarias al marco acordado por todos los Estados Miembros de las Naciones Unidas. Australia anima a la comunidad mundial a poner de manifiesto las actividades cibernéticas malintencionadas y a pedir cuentas a los responsables. Australia tiene la política de atribuir públicamente la ciberactividad maliciosa cuando se conoce el origen y cuando nos interesa hacerlo. Esta política no está dirigida a ningún país en particular. Hasta la fecha, Australia ha atribuido públicamente ciberactividad maliciosa en 13 ocasiones. Más recientemente, el 10 de mayo de 2022, Australia se unió a los Estados Unidos de América y a la Unión Europea para atribuir al Gobierno ruso una serie de actividades cibernéticas destructivas, perturbadoras y desestabilizadoras contra Ucrania.

Participación de múltiples interesados

Australia agradece a Burhan Gafoor, Presidente 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, sus constructivos esfuerzos por obtener un acuerdo consensuado sobre un conjunto de modalidades transparentes y equilibradas para la futura participación de las partes interesadas no gubernamentales en el grupo de trabajo. Australia espera que estas modalidades se adopten formalmente en el tercer período de sesiones sustantivo del grupo de trabajo, que se celebrará en julio de 2022. Australia es un firme partidario de la participación de las múltiples partes interesadas en los debates sobre el comportamiento responsable de los Estados en el ciberespacio. El ciberespacio es único: el sector privado, la comunidad técnica, la sociedad civil y el mundo académico desempeñan un papel vital en su gestión técnica y su gobernanza, y la comunidad de múltiples partes interesadas puede aportar perspectivas que nos ayuden a comprender mejor las ciberamenazas emergentes, sus repercusiones y la forma de abordarlas. Australia se sintió decepcionada por los esfuerzos de algunos Estados por obstaculizar la participación de las partes interesadas en el proceso, lo que consideramos que va en contra del espíritu con el que se creó el grupo de trabajo. Australia cree que el grupo de trabajo puede tener un impacto de gran alcance en muchas partes interesadas, incluyendo impactos directos en las comunidades y los individuos, y que abordar las amenazas que emanan del ciberespacio requiere que aprovechemos la experiencia, los conocimientos y los recursos de todas las partes interesadas pertinentes. Por lo tanto, Australia acoge con

satisfacción las modalidades acordadas como un paso hacia la transparencia y la inclusión.

Las mujeres en el ciberespacio

Tal y como se reconoce en la agenda sobre las mujeres y la paz y la seguridad, las mujeres y las niñas se ven afectadas de forma única y desproporcionada por los conflictos y las crisis, además de estar infrarrepresentadas en los procesos internacionales de paz y seguridad (y excluidas de ellos). Tal y como se señala en el informe del UNIDIR "Still behind the curve: gender balance in arms control, non-proliferation and disarmament diplomacy", los procesos de la Primera Comisión van muy por detrás de los avances hacia la paridad de género que se observan en otras comisiones de las Naciones Unidas. Los datos del UNIDIR muestran que, en los debates de la Primera Comisión, el 27% de los oradores son mujeres. Esta cifra se reduce a una media del 20% en los foros sobre temas más especializados.

Para abordar esta cuestión, Australia, junto con Canadá, los Países Bajos, Nueva Zelanda, el Reino Unido de Gran Bretaña e Irlanda del Norte y los Estados Unidos, pusieron en marcha en febrero de 2020 la Beca de Mujeres en la Seguridad Internacional y el Ciberespacio. La beca ofrece a las mujeres diplomáticas que inician su carrera profesional una formación en materia de negociaciones multilaterales, ciberpolítica y derecho internacional, y patrocina el viaje a Nueva York para que se unan a sus delegaciones nacionales en las reuniones de las Naciones Unidas en las que se estudia el comportamiento responsable de los Estados en el ciberespacio, incluido el grupo de trabajo.

Australia se complace de que, gracias a la beca, muchos becarios hayan podido unirse a sus delegaciones nacionales en las sesiones primera y segunda del grupo de trabajo y hayan contribuido de forma significativa al grupo de trabajo y al avance de la agenda sobre las mujeres y la paz y la seguridad. En la primera sesión del grupo de trabajo, celebrada en diciembre de 2021, el 37% de las intervenciones fueron realizadas por mujeres. En su segunda sesión, celebrada en marzo de 2022, el 43% de las intervenciones, y la mitad de todas las declaraciones de derecho internacional, fueron realizadas por mujeres.

Azerbaiyán

[Original: inglés]
[31 de mayo de 2022]

En los últimos años, se han adoptado en Azerbaiyán varias leyes nuevas para garantizar la seguridad de la información. Además, se han adoptado el concepto de desarrollo, la hoja de ruta estratégica, la estrategia nacional y los programas estatales, y se ha establecido la cooperación con varios países mediante decretos y órdenes del Presidente de Azerbaiyán.

Debido a la necesidad de considerar la seguridad de las infraestructuras de información críticas como una prioridad, se adoptó un acto jurídico normativo para reforzar la seguridad en este ámbito. La clasificación de estas instalaciones de infraestructura en función de su importancia y la determinación de los requisitos de seguridad generales y especiales se tienen en cuenta en el mencionado acto jurídico, y está previsto que se lleve a cabo un control continuo mediante la aplicación de métodos adecuados.

El Comité de Coordinación de la Seguridad de la Información se creó en 2018, en virtud de la orden del Presidente de Azerbaiyán.

Con el fin de mantener la seguridad de las infraestructuras de información críticas, se ha determinado la división de poderes entre las instituciones de acuerdo con el decreto del Presidente de Azerbaiyán de 17 de abril de 2021.

Con el fin de mejorar el capital humano en este campo, la Academia Cibernética del Ministerio de Desarrollo Digital y Transporte organizó varias sesiones de capacitación, en las que se proporcionaron certificados nacionales e internacionales.

Expertos internacionales celebraron seminarios virtuales sobre la protección de datos personales, la ciberdelincuencia y las pruebas electrónicas para los representantes de los organismos estatales pertinentes de Azerbaiyán, en el marco de los programas conjuntos CyberEast y Cybersecurity East de la Unión Europea y el Consejo de Europa.

Representantes de varios organismos estatales de Azerbaiyán asistieron a su primera formación certificada sobre ciberseguridad, en el marco del programa de subvenciones de la Agencia de Cooperación Internacional de la República de Corea.

Además de lo anterior, se han llevado a cabo consultas e iniciativas de cooperación con los equipos de respuesta a emergencias informáticas de varios Estados.

Azerbaiyán ocupa el cuadragésimo lugar del mundo y el tercero (tras la Federación de Rusia y Kazajstán) de la Comunidad de Estados Independientes en el índice mundial de ciberseguridad de 2020 de la Unión Internacional de Telecomunicaciones.

Debido al aumento del número de ciberamenazas durante la pandemia de enfermedad por coronavirus (COVID-19), así como a las deficiencias detectadas en los programas y equipos técnicos, se han publicado notificaciones y mensajes pertinentes sobre los métodos de protección contra las ciberamenazas en www.cert.az y en las redes sociales.

Cuba

[Original: español]
[31 de mayo de 2022]

El uso indebido de las tecnologías de la información y las telecomunicaciones sigue siendo un asunto de gran preocupación para la comunidad internacional, de ahí la necesidad de hacer frente a las crecientes amenazas en ese ámbito.

Condenamos el uso indebido de las plataformas de los medios de comunicación, incluidas las redes sociales y las emisiones de radio, como herramienta para el intervencionismo a través de la promoción del discurso del odio, la incitación a la violencia, la subversión, la desestabilización, la difusión de noticias falsas y la tergiversación de la realidad con fines políticos y como pretexto para hacer la guerra o para la amenaza o el uso de la fuerza, en violación de los propósitos y principios de la Carta de las Naciones Unidas y del derecho internacional.

En este sentido, rechazamos los métodos de guerra no convencionales desplegados por el Gobierno de Estados Unidos contra Cuba, incluso mediante el uso de las nuevas tecnologías de la información y otras plataformas digitales para desestabilizar y desacreditar a nuestro país.

Reafirmamos el derecho y el deber que tienen los Estados de combatir, como prerrogativa constitucional, la difusión de noticias falsas o distorsionadas que pudieran interpretarse como una injerencia en los asuntos internos de otros Estados o

como perjudiciales para la promoción de la paz, la cooperación y las relaciones amistosas entre Estados y naciones,

No podemos ignorar el hecho de que el creciente desarrollo de capacidades y operaciones ciberofensivas puede transformar el ciberespacio en un nuevo escenario de conflicto. Rechazamos los intentos de equiparar el uso malicioso de las tecnologías de la información y las comunicaciones con el concepto de “ataque armado” para justificar el ejercicio del derecho de legítima defensa previsto en el artículo 51 de la Carta de las Naciones Unidas.

Repudiamos el uso deliberado de estas tecnologías para dañar las infraestructuras vitales de otros Estados, incluidos sus sistemas de información, o para obstaculizar de otro modo el uso y el funcionamiento de las infraestructuras críticas, que son esenciales para la estabilidad social y la seguridad de los Estados.

Las Naciones Unidas son el foro multilateral por excelencia y la principal plataforma para abordar las preocupaciones de sus Estados miembros en materia de seguridad y uso de las tecnologías de la información y las comunicaciones. A este respecto, 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, creado en virtud de la resolución 75/240 de la Asamblea General, es el único mecanismo inclusivo de que disponen los Estados miembros para debatir las cuestiones de ciberseguridad de forma transparente y en pie de igualdad.

Reiteramos la importancia del mencionado grupo de trabajo y esperamos que este proceso intergubernamental contribuya a llenar el vacío jurídico existente con normas vinculantes que conduzcan a la adopción de un instrumento jurídico global sobre las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

Aunque las medidas de fomento de la confianza son una herramienta útil, estas medidas no garantizan por sí solas el uso estrictamente pacífico de las tecnologías de la información y las comunicaciones, dado que no existe ningún instrumento jurídicamente vinculante en este ámbito.

Cuba, como miembro del Movimiento de Países No Alineados, exhorta una vez más a los países desarrollados y a las entidades internacionales pertinentes a brindar a los países en desarrollo que lo soliciten, asistencia y cooperación, incluso mediante recursos financieros, creación de capacidades y transferencia de tecnología, teniendo en cuenta las necesidades y características específicas de cada Estado receptor.

Nos oponemos a la aplicación de medidas coercitivas unilaterales que, como el bloqueo económico, comercial y financiero impuesto por el Gobierno de Estados Unidos contra Cuba, impiden o limitan el acceso universal y el uso y disfrute pacífico de las tecnologías de la información y las comunicaciones para el bienestar de nuestras poblaciones.

Dinamarca

[Original: inglés]
[31 de mayo de 2022]

En Dinamarca, como en muchas partes del mundo, las soluciones digitales constituyen una parte esencial de la vida cotidiana. Son tanto una plataforma para las actividades sociales básicas como un motor clave del crecimiento económico. Sin embargo, a medida que nuestras sociedades y nuestra infraestructura digital están cada vez más interconectadas, también ha aumentado la capacidad y la voluntad de los agentes estatales y no estatales de llevar a cabo actividades cibernéticas

maliciosas. Esto debería ser motivo de preocupación a nivel mundial, ya que las actividades maliciosas en el ciberespacio pueden constituir actos ilícitos en virtud del derecho internacional y conducir a una posible escalada, que a su vez amenaza la seguridad y la estabilidad internacionales. La invasión no provocada e ilegal de Ucrania por parte de Rusia, que también incluye ciberataques contra infraestructuras críticas, es especialmente preocupante y completamente inaceptable, ya que constituye una violación del derecho internacional y socava el marco del comportamiento responsable de los Estados en el ciberespacio.

Como uno de los países más digitalizados del mundo, Dinamarca sigue decidida a prevenir, disuadir y responder en consecuencia a las actividades maliciosas y a potenciar la cooperación internacional a tal efecto. Dinamarca, conjuntamente con la Unión Europea, busca reforzar la cooperación internacional en favor de un ciberespacio mundial, abierto, estable, pacífico y seguro en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el estado de derecho. A este respecto, Dinamarca subraya la importancia de que los Estados se adhieran al marco de comportamiento estatal responsable en el ciberespacio, que apoya el orden internacional basado en normas, y afirma la aplicabilidad del derecho internacional, la adhesión a las normas voluntarias de comportamiento estatal responsable y el desarrollo y la aplicación de medidas prácticas de fomento de la confianza. Todos los miembros de la Asamblea General han afirmado repetidamente que el marco es la piedra angular de los esfuerzos de la comunidad internacional para disuadir el comportamiento imprudente e irresponsable de los Estados en el ciberespacio y evitar los ciberataques más perjudiciales y las posibles escaladas. Por ello, pedimos a todos los Estados miembros, incluida la Federación de Rusia, que cumplan sus compromisos.

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito

Hasta ahora, Dinamarca ha adoptado varias medidas para fortalecer su ciberseguridad y la seguridad de la información y para promover la cooperación internacional en la ciberseguridad. El Acuerdo de Defensa danés para el período 2018-2023 destina 1.400 millones de coronas al refuerzo de la ciberseguridad y la ciberdefensa, reforzando así la resiliencia y la solidez de la sociedad danesa frente a los ciberataques.

Con la estrategia danesa de ciberseguridad y seguridad de la información para el periodo 2018-2021, se introdujeron 25 iniciativas, así como 6 estrategias dedicadas, con el objetivo de:

a) Aumentar la ciberseguridad y la seguridad de la información, especialmente en los sectores críticos;

b) Garantizar esfuerzos sistemáticos y coordinados;

c) Mejorar la resiliencia tecnológica de las infraestructuras digitales;

d) Mejorar los conocimientos de los ciudadanos, las empresas y las autoridades en materia de ciberseguridad.

Como parte de la estrategia, se crearon unidades dedicadas a la ciberseguridad y la seguridad de la información en los seis sectores críticos (energía, finanzas, transporte, sanidad, telecomunicaciones y marítimo), así como foros para que las unidades compartan experiencias.

El Centro de Ciberseguridad también ha puesto en marcha su propia Academia Cibernética intensiva y apoya ampliamente la educación y la investigación en el campo de la ciberseguridad. Asimismo, la Agencia para el Gobierno Digital desarrolló

varios cursos, materiales didácticos y eventos sobre ciberseguridad y seguridad de la información dirigidos a jefes de gobierno, ciberespecialistas y empleados públicos.

Además, la Agencia para el Gobierno Digital ha desarrollado el sitio web www.sikkerdigital.dk, que ofrece orientaciones concretas sobre ciberseguridad y seguridad de la información a los ciudadanos y lleva a cabo campañas nacionales sobre comportamiento digital seguro en estrecha colaboración con municipios y regiones.

Dinamarca ha creado un Consejo de Ciberseguridad público-privado (Cybersikkerhedsråd), que asesora al Gobierno sobre cómo reforzar la ciberseguridad y mejorar el intercambio de conocimientos entre autoridades, empresas e investigadores. Por último, con la estrategia danesa de ciberseguridad y seguridad de la información para el periodo 2018-2021, Dinamarca también reforzó su compromiso cibernético internacional, lo que permitió al país intensificar su participación en ciberforos multinacionales como las Naciones Unidas, la Unión Europea, la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Seguridad y la Cooperación en Europa (OSCE).

En diciembre de 2021, el Gobierno presentó una nueva estrategia nacional de ciberseguridad y seguridad de la información para 2022-2024. La estrategia se basa en los esfuerzos actuales y los amplía reforzando la ciberseguridad y la seguridad de la información a través de 34 iniciativas principales dirigidas a los sectores público y privado, así como a los ciudadanos daneses en general. En general, la estrategia incluye cuatro objetivos principales:

a) En primer lugar, la estrategia refuerza aún más la resistencia de las infraestructuras críticas de las tecnologías de la información y la comunicación (TIC) que sustentan las funciones vitales de la sociedad. Para garantizar un nivel adecuado de ciberseguridad tanto para los organismos públicos como para las empresas, se ha puesto en marcha una serie de acciones estratégicas, entre las que se incluyen el endurecimiento de los requisitos de seguridad para la gestión de los sistemas de TIC gubernamentales críticos para la sociedad y el refuerzo de la respuesta policial a la ciberdelincuencia. La estrategia también amplía el número de sectores críticos para incluir una gama más amplia de organismos públicos con responsabilidad sobre las funciones sociales vitales apoyadas por las tecnologías de la información. Los organismos públicos de estos sectores críticos deben cumplir una serie de requisitos de seguridad específicos, además de los requisitos mínimos que se introdujeron anteriormente en la estrategia 2018-2021. Se trata de garantizar que los ministerios con una responsabilidad especial sobre funciones sociales vitales puedan actuar con rapidez y eficacia en caso de un ciberincidente grave;

b) En segundo lugar, la estrategia incluye una serie de iniciativas que refuerzan los conocimientos de los ciudadanos daneses en materia de ciberseguridad y aumentan el compromiso de la dirección con el fortalecimiento de la ciberseguridad. Entre las iniciativas se encuentran nuevos programas de capacitación para los empleados públicos, así como programas educativos que dotan a niños, jóvenes y adultos de las competencias necesarias para estar alfabetizados digitalmente. Además, los altos directivos y líderes se enfrentan a mayores exigencias y expectativas para dar prioridad a la ciberseguridad y la seguridad de la información;

c) En tercer lugar, la estrategia refuerza la cooperación en materia de ciberseguridad y seguridad de la información entre los sectores público y privado. La capacidad de compartir conocimientos y experiencias entre sectores es vital para lograr un alto nivel de ciberseguridad y seguridad de la información. Por este motivo, se creará una ciberlínea, que facilitará la búsqueda de asesoramiento en relación con la ciberdelincuencia, así como una unidad de ciberseguridad dedicada a las pequeñas

y medianas empresas, con el fin de reforzar la capacidad del Centro de Ciberseguridad para proporcionar orientación;

d) En cuarto lugar, la estrategia refuerza aún más los esfuerzos internacionales de Dinamarca en materia de ciberseguridad. Esto incluye la asignación de recursos adicionales a su servicio diplomático para reforzar la contribución del país a la cooperación multilateral en materia de ciberseguridad en el seno de la Unión Europea, la OTAN y las Naciones Unidas y para promover la cooperación con la industria tecnológica internacional, el mundo académico y los grupos de reflexión, así como los controles de las exportaciones de productos digitales. Por último, la estrategia también incluye iniciativas que reforzarán los esfuerzos nacionales e internacionales del país para establecer ciberdefensas activas y aumentar la disuasión.

Además de las iniciativas puestas en marcha en el marco de las estrategias nacionales de ciberseguridad y seguridad de la información, Dinamarca continúa su amplio compromiso en la lucha contra las amenazas híbridas, como los ciberataques y las operaciones de influencia, mediante la colaboración con sus socios y aliados de la OTAN y la Unión Europea. Dinamarca también contribuye a los esfuerzos diplomáticos en el seno de las Naciones Unidas, la Unión Europea, la OTAN y la OSCE con el fin de promover sistemáticamente un ciberespacio libre, abierto, estable, pacífico y seguro.

En particular, Dinamarca apoya la idea de establecer un programa de acción de las Naciones Unidas que podría proporcionar una plataforma para que los Estados y los actores no estatales cooperen más, por ejemplo, en lo que respecta a la puesta en marcha de actividades de creación de capacidades adaptadas a sus necesidades o al avance de sus esfuerzos nacionales de aplicación en el marco de las Naciones Unidas, lo que daría lugar a una mayor resiliencia y estabilidad colectiva en el ámbito de las TIC.

Además, Dinamarca también es miembro activo del Grupo de Cooperación de Redes y Sistemas de Información y de la red de equipos de respuesta a incidentes de ciberseguridad, y forma parte del consejo de la Agencia de la Unión Europea para la Ciberseguridad.

Contenido de los conceptos mencionados en el informe 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 y los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

Amenazas actuales y emergentes

Dinamarca reconoce que el ciberespacio ofrece enormes oportunidades para aumentar el bienestar, impulsar el crecimiento económico sostenible y mejorar la calidad de vida de nuestros ciudadanos. No obstante, nuestra dependencia de las soluciones digitales también crea ciertos desafíos y vulnerabilidades.

Dinamarca está preocupada por el aumento de las actividades malintencionadas en el ciberespacio por parte de agentes estatales y no estatales, así como por el aumento del robo de propiedad intelectual facilitado por medios cibernéticos. Tales acciones amenazan el crecimiento económico y la estabilidad de la comunidad internacional.

Los actores estatales y no estatales han demostrado su voluntad de aprovechar cualquier oportunidad para llevar a cabo ciberactividades maliciosas. Esto incluye la

interferencia en infraestructuras críticas y el robo cibernético de la propiedad intelectual. Cualquier intento de obstaculizar la capacidad de la infraestructura crítica es inaceptable y puede poner en peligro la vida de las personas. Dinamarca está especialmente alarmada por el reciente aumento de las actividades que afectan a la seguridad e integridad de los productos y servicios de las TIC, que podrían tener efectos sistémicos. En concreto, el uso por parte de Rusia de ciberataques contra infraestructuras críticas como parte de la invasión no provocada e ilegal de Ucrania es completamente inaceptable y, por tanto, debe ser condenado enérgicamente por toda la comunidad internacional. Los Estados deben abstenerse de utilizar los ciberataques, ejercer la debida diligencia y tomar medidas rápidas y firmes contra las actividades maliciosas de las TIC que se originen en su territorio, en consonancia con el derecho internacional y los informes de consenso de 2010, 2013, 2015 y 2021 de los Grupos de Expertos Gubernamentales y el informe del Grupo de Trabajo en 2021.

Como se ha reconocido en anteriores informes del Grupo de Expertos Gubernamentales, así como en el informe del Grupo de Trabajo, dado el carácter único de las TIC, el enfoque de las Naciones Unidas y de sus Estados Miembros para abordar las cuestiones cibernéticas en el contexto de la seguridad internacional debe seguir siendo tecnológicamente neutro. Esto es coherente con el concepto y con el reconocimiento por parte de las Naciones Unidas de que el derecho internacional vigente se aplica a nuevas esferas, incluido el uso de tecnologías emergentes.

Forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones

Dinamarca apoya firmemente un sistema multilateral basado en el orden internacional basado en normas para hacer frente a las amenazas existentes y potenciales derivadas del uso malintencionado de las TIC.

Como se reconoce en los informes de consenso de los Grupos de Expertos Gubernamentales de 2010, 2013, 2015 y 2021, así como en los principios establecidos en el párrafo 71 (b) a (g) del informe de 2021 y del Grupo de Trabajo, la comunidad internacional ha dejado muy claro que el ciberespacio está firmemente arraigado en el derecho internacional vigente. Dinamarca pone de relieve que el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplica al comportamiento de los Estados en el ciberespacio. Por ello, pedimos a todos los Estados miembros que cumplan el compromiso.

La soberanía, la no intervención y la prohibición del uso de la fuerza son principios fundamentales del derecho internacional, y su violación por parte de los Estados puede constituir un hecho internacionalmente ilícito, para el cual los Estados podrán adoptar contramedidas y pedir reparación en virtud de las normas de responsabilidad del Estado. Todavía se puede reforzar la comprensión e interpretación común de estos principios fundamentales. Dinamarca apoya la labor del Grupo de Expertos Gubernamentales y del Grupo de Trabajo, así como otras iniciativas internacionales y regionales, incluido el programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio, en la búsqueda de este resultado.

Es importante que los Estados no utilicen el principio de soberanía para limitar o violar el derecho internacional de los derechos humanos dentro de sus propias fronteras. El derecho de los derechos humanos es aplicable tanto en línea como fuera de ella, y entraña una obligación tanto negativa como positiva para los Estados de abstenerse de actos que violen los derechos humanos, y el deber de garantizar que las personas puedan ejercer sus derechos y libertades.

Como se describe en el manual militar de Dinamarca, las operaciones en el ciberespacio no difieren del uso de capacidades militares convencionales en relación con el derecho internacional aplicable. La cuestión también se refleja en la Doctrina Conjunta nacional para Operaciones Militares en el Ciberespacio de 2019, según la cual los dirigentes militares están obligados a incluir consideraciones sobre el cumplimiento del derecho internacional al realizar operaciones en el ciberespacio. Así pues, el derecho internacional humanitario, incluidos los principios de precaución, humanidad, necesidad militar, proporcionalidad y distinción, se aplica a la conducta de los Estados en el ciberespacio y es totalmente protector, al establecer límites claros para su legalidad, en tiempos de conflicto armado. Dinamarca desea sumarse a la Unión Europea para subrayar que el derecho internacional no es un factor que propicia los conflictos, sino una forma de proteger a los civiles y limitar los efectos desproporcionados.

El derecho internacional vigente —complementado por las 11 normas voluntarias y no vinculantes para el comportamiento responsable de los Estados incluidas en el informe del Grupo de Expertos Gubernamentales de 2015— proporciona a los Estados un marco para el comportamiento responsable en el ciberespacio. Dinamarca exhorta a todos los Estados a que se adhieran a este marco y apliquen sus recomendaciones.

Como el derecho internacional vigente se aplica en el ciberespacio, Dinamarca no pide ni ve la necesidad de nuevos instrumentos jurídicos internacionales para las cuestiones relativas al ciberespacio. Sin embargo, hay margen para fortalecer el entendimiento común de cómo el derecho internacional vigente se aplica a las cuestiones relativas a esos temas. Dinamarca espera que el trabajo y las recomendaciones del Grupo de Trabajo contribuyan a nuevas aclaraciones y faciliten así el cumplimiento de los Estados, además de promover una mayor previsibilidad y reducir el riesgo de escalada. Para ello, Dinamarca trabaja actualmente en la elaboración de una posición nacional sobre la aplicación del derecho internacional a la actuación de los Estados en el ciberespacio.

Normas, reglas y principios de comportamiento responsable de los Estados

Dinamarca se une a la Unión Europea y a sus Estados miembros para alentar a todos los Estados a que se basen en la labor respaldada reiteradamente por la Asamblea General, en particular en su resolución 76/19, y a que apliquen las normas acordadas sobre el comportamiento responsable de los Estados en el ciberespacio, así como las medidas de fomento de la confianza, que desempeñan un papel esencial en la prevención de conflictos. Acogemos con satisfacción un diálogo inclusivo y constructivo en el seno del Grupo de Trabajo, así como la posibilidad de una cooperación práctica a través de un posible programa de acción de las Naciones Unidas.

Como complementarias del derecho internacional vinculante y derivadas de este, las normas, reglas y principios de comportamiento responsable de los Estados establecidos en los sucesivos informes del Grupo de Expertos Gubernamentales en 2010, 2013, 2015 y 2021, así como el informe del Grupo de Trabajo, tienen un inmenso valor. Dinamarca seguirá guiándose por el derecho internacional, así como por la adhesión a estas normas, reglas y principios voluntarios. La aplicación ulterior de esas normas debería llevarse a cabo mediante una mayor cooperación y transparencia en torno a las mejores prácticas.

Medidas de fomento de la confianza

La creación de mecanismos eficaces de cooperación entre los Estados en materia de ciberseguridad es fundamental para el intercambio de información, la creación de

confianza y la prevención de conflictos. Los foros regionales, como la OSCE, ya han establecido plataformas relevantes para las medidas de fomento de la confianza y la cooperación entre los actores con preocupaciones compartidas e intereses comunes para abordar eficazmente los desafíos desde una perspectiva regional. Además, el propio Grupo de Trabajo debe considerarse como una medida de fomento de la confianza, ya que proporciona un foro internacional para que todos los Estados miembros intercambien información y compartan sus puntos de vista sobre las cuestiones cibernéticas.

Dinamarca se une a la Unión Europea y a sus Estados miembros para animar a la comunidad internacional a seguir desarrollando y aplicando medidas de fomento de la ciberconfianza que aumenten la previsibilidad del comportamiento de los Estados y reduzcan el riesgo de interpretaciones erróneas, escaladas y conflictos, contribuyendo así a la estabilidad a largo plazo en el ciberespacio.

Cooperación y asistencia internacionales en materia de seguridad y fomento de la capacidad en el ámbito de las tecnologías de la información y las comunicaciones

Reforzar la ciberresiliencia de nuestras sociedades es crucial para reducir los riesgos derivados del uso malintencionado de las TIC, reducir las tensiones y prevenir los conflictos. Por lo tanto, como se ha señalado anteriormente, el Gobierno de Dinamarca ha introducido un amplio número de iniciativas para reforzar la ciberresiliencia nacional. Del mismo modo, la Unión Europea y sus Estados miembros, entre ellos Dinamarca, también están cooperando para reforzar la capacidad de recuperación en toda la Unión Europea, especialmente a través de las directivas sobre la seguridad de las redes y los sistemas de información.

Además de estos esfuerzos, Dinamarca -junto con la Unión Europea y sus Estados miembros- también contribuye a aumentar la ciberresiliencia de los países en desarrollo a través de una serie de programas e iniciativas a medida, cuyo objetivo es desarrollar las habilidades y capacidades para hacer frente a los ciberincidentes, así como facilitar el intercambio de mejores prácticas.

Dinamarca se une a la Unión Europea y a sus Estados miembros en el reconocimiento de que la promoción de una infraestructura digital más resiliente contribuirá a un ciberespacio más seguro y estable, y anima a todos los actores relevantes a comprometerse en la creación de capacidades a este respecto y a pedir una mayor cooperación con los principales socios y organizaciones internacionales para apoyar la creación de capacidades en terceros países.

Además, Dinamarca también apoya el establecimiento de un mecanismo de las Naciones Unidas para fomentar programas de creación de capacidades adaptados a las necesidades identificadas por los Estados beneficiarios, como el programa de acción, y la identificación de mecanismos que faciliten el compromiso de todas las partes interesadas en la aplicación del marco de comportamiento responsable.

Egipto

[Original: árabe]
[31 de mayo de 2022]

Opiniones y propuestas egipcias para reforzar la seguridad de la información y promover la cooperación internacional

I. Iniciativas nacionales

- En los últimos tiempos, Egipto ha reforzado sus esfuerzos de capacitación y ha desarrollado marcos normativos para la seguridad de las comunicaciones y de

la información, de acuerdo con las recomendaciones de los informes finales del grupo de trabajo de composición abierta y los informes del Grupo de Expertos Gubernamentales.

- El Estado egipcio está adoptando políticas equilibradas para estar al día y combatir la ciberdelincuencia y hacer frente a las actividades ilegales en Internet y las redes sociales de acuerdo con un marco legislativo basado en una serie de leyes de reciente creación, entre las que se encuentran las siguientes: la Ley núm. 175 (2018) sobre la lucha contra los delitos informáticos, la Ley núm. 180 (2018) sobre la regulación de la prensa y los medios de comunicación y la Ley núm. 151 (2020) sobre la protección de los datos personales.
- Se ha creado el Consejo Superior de Ciberseguridad como autoridad competente y referencia nacional en materia de ciberseguridad. Se lanzó una estrategia nacional de ciberseguridad como parte de la Visión 2030 de Egipto. Establecerá un sistema nacional integrado que incorpore las mejores prácticas internacionales. Creará asociaciones nacionales de ciberseguridad entre los organismos gubernamentales y el sector privado y reforzará los programas de ciberdefensa mediante el establecimiento y la mejora de la eficacia de los equipos y redes de respuesta a emergencias informáticas formados en diversos sectores del Estado. También creará y desarrollará programas de concienciación sobre ciberseguridad dirigidos a grupos sociales concretos, como los escolares, las administraciones públicas y los ancianos, y promoverá la investigación y la innovación científica en materia de ciberseguridad.
- Se han adoptado una serie de políticas nacionales, mecanismos de gobernanza y marcos y normas reguladoras. Incluyen controles básicos de ciberseguridad, controles de los sistemas de ciberseguridad y una supervisión continua de la ciberseguridad a nivel nacional.
- Egipto se esfuerza por promover la cooperación internacional bilateral y multilateral en materia de seguridad de la información y creación de capacidades.
- Se han puesto en marcha numerosos programas e iniciativas nacionales para sensibilizar a la población, prevenir los ciberriesgos y reducir su impacto mediante la emisión de alertas sobre las últimas y más peligrosas cibervulnerabilidades.
- Se está cooperando con organismos y academias nacionales para desarrollar capacidades y crear una reserva cualificada de personal de ciberseguridad y seguridad de la información.

II. Propuestas

- Es crucial reforzar la cooperación internacional en materia de ciberseguridad para minimizar las ciberactividades delictivas transfronterizas y prevenir la comisión de ciberdelitos. También debemos intercambiar conocimientos y tecnologías modernas para perseguir todos los usos ilegales de Internet, de modo que los Estados puedan hacerles frente. Deben impartirse cursos de formación para desarrollar las capacidades de los organismos de seguridad encargados de combatir la ciberdelincuencia.
- Deben tomarse medidas para regular la circulación de las criptomonedas, de modo que no se utilicen para financiar actividades ilegales. También debería considerarse la creación de una unidad especializada en ciberdelincuencia en la Organización Internacional de Policía Criminal-INTERPOL para facilitar el

intercambio de información entre los organismos de seguridad que participan en la lucha contra estas actividades.

Federación de Rusia

[Original: ruso]
[31 de mayo de 2022]

El siglo XXI ha sido una época de avances en el campo de la tecnología de la información, que ha conquistado prácticamente todos los aspectos de nuestra vida. Los sectores tradicionales de la administración, el público y las empresas están experimentando una completa transformación. Han surgido nuevas oportunidades para hacer crecer la economía, crear empleo y mejorar la calidad de vida de todos. Sin embargo, las nuevas tecnologías han venido acompañadas de nuevos retos.

El espacio digital global se ha convertido en escenario frecuente de despiadadas guerras de información, ataques informáticos, incluso contra infraestructuras de información críticas, y competencia desleal y uso indebido por parte de empresas privadas. Entre las principales amenazas se encuentra el uso de las tecnologías de la información y las comunicaciones (TIC) en los ámbitos militar, político y otros para socavar la soberanía, violar la integridad territorial e interferir en los asuntos internos de los Estados; la difusión de programas maliciosos a través de códigos abiertos; y el uso de las TIC con fines terroristas, extremistas o delictivos. Estas amenazas han cambiado fundamentalmente el mundo y han puesto en riesgo la seguridad internacional.

Rusia fue uno de los primeros países en pedir a la comunidad internacional que aunara esfuerzos en este nuevo ámbito. En 1998, a iniciativa nuestra, la Asamblea General adoptó una resolución sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. La resolución era un llamamiento a la cooperación más amplia posible para combatir las amenazas comunes en la esfera de la información, en primer lugar los intentos de utilizar las últimas tecnologías de la información para socavar la paz y la estabilidad internacionales. Nuestros esfuerzos han incluido el tema de la seguridad de la información en el programa de la Asamblea General y han conseguido que la resolución sobre seguridad de la información internacional tenga lugar cada año.

Rusia también estuvo detrás de la iniciativa, en 2004, de crear el Grupo de Expertos Gubernamentales, el primer foro de expertos de las Naciones Unidas de este tipo para debatir los aspectos de seguridad de las TIC. Desde entonces, ha habido seis Grupos de Expertos Gubernamentales. La rápida evolución del espacio informativo ha permitido llevar los debates a un nivel completamente nuevo.

En 2018, la mayoría de los Estados miembros de las Naciones Unidas votaron a favor de la resolución sobre seguridad de la información internacional patrocinada por Rusia. La resolución establece un primer conjunto de reglas, normas y principios para un comportamiento estatal responsable en relación con el uso de las TIC. La Asamblea General también decidió convocar un grupo de trabajo de composición abierta, con el fin de seguir desarrollando esa lista y, en general, conducir el debate sobre la seguridad de la información internacional de una manera más democrática. El grupo completó su trabajo y los Estados miembros adoptaron su informe final por consenso el 12 de marzo de 2021, en Nueva York.

Rusia colaboró con delegaciones afines para garantizar la continuidad del proceso de negociación bajo los auspicios de las Naciones Unidas mediante la creación de un nuevo grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). El

mandato del grupo es seguir desarrollando las reglas, normas y principios del comportamiento responsable de los Estados y las formas de su aplicación. El grupo de trabajo lo hará principalmente alcanzando un entendimiento común de las amenazas a la seguridad de la información, la aplicabilidad del derecho internacional al uso de las TIC por parte de los Estados, las medidas de fomento de la confianza y de la capacidad, y fortaleciendo los vínculos entre los organismos pertinentes. El grupo se encarga de que los Estados tengan un papel destacado en el debate y ofrece a las organizaciones no gubernamentales la oportunidad de participar.

La Federación de Rusia adopta un enfoque transparente y coherente para garantizar la seguridad de la información internacional. La seguridad de la información internacional fue designada como prioridad nacional estratégica en la estrategia de seguridad nacional de la Federación de Rusia, aprobada por el Decreto Presidencial núm. 400 de 2 de julio de 2021. De acuerdo con el marco de la política estatal de la Federación de Rusia en el ámbito de la seguridad de la información internacional, aprobado por el Decreto Presidencial núm. 213 de 12 de abril de 2021, el objetivo de la política estatal es promover el establecimiento de un régimen jurídico internacional que regule el espacio global de la información.

Creemos que los acuerdos universales jurídicamente vinculantes son necesarios para prevenir conflictos y fomentar una cooperación mutuamente beneficiosa en el espacio de la información. El proyecto de convención sobre la lucha contra el uso de las TIC con fines delictivos, presentado por Rusia en el comité especial creado a iniciativa nuestra, podría servir de base para tales acuerdos, al igual que la propuesta rusa de una convención de las Naciones Unidas sobre la seguridad de la información internacional.

Las TIC deben estar al servicio de los objetivos de desarrollo sostenible y permitir condiciones favorables para la investigación científica y la rápida aplicación de soluciones técnicas. Con el fin de garantizar que estos principios se incorporen a futuras obligaciones legales universalmente acordadas y equitativas, en 2021, Rusia y los Estados Unidos de América iniciaron la adopción de la resolución 76/19 de la Asamblea General, por consenso, y 108 Estados miembros se sumaron a la lista de patrocinadores.

Rusia cree en la inviolabilidad de la soberanía digital de los Estados. Cada país puede y debe establecer sus propios parámetros para regular su espacio de información y la infraestructura relacionada. Rusia insiste en la internacionalización y la igualdad de derechos de los Estados en la gobernanza de Internet. Cualquier intento de limitar el derecho soberano de los Estados a regular y asegurar los segmentos nacionales de la red mundial es inaceptable.

Es importante que se establezcan medidas legales a nivel nacional o internacional para evitar que ciertos Estados dominen la esfera digital. Es importante tomar medidas para garantizar que los derechos de todos los usuarios del espacio informativo reciban una protección fiable e igualitaria. Ningún Estado o grupo de países puede establecer unilateralmente principios, reglas y normas para el funcionamiento de Internet. Para ello, Rusia insiste en que la gobernanza de Internet sea competencia de la Unión Internacional de Telecomunicaciones, un organismo especializado de las Naciones Unidas con los conocimientos necesarios en el ámbito de las telecomunicaciones y las TIC.

Como antes, Rusia está abierta al diálogo y a la cooperación constructiva con todos sus socios, tanto a nivel bilateral como a través de los organismos y foros internacionales, principalmente, en las Naciones Unidas.

Singapur

[Original: inglés]
[31 de mayo de 2022]

Singapur está firmemente comprometido con el reforzamiento de un orden internacional basado en normas en el ciberespacio que sirva de base para la confianza entre los Estados miembros y facilite el progreso económico y social. Para aprovechar plenamente los beneficios de las tecnologías digitales, la comunidad internacional debe crear un ciberespacio seguro, fiable, abierto e interoperable, basado en el derecho internacional aplicable, normas bien definidas de comportamiento responsable de los Estados, medidas sólidas de fomento de la confianza y creación de capacidades coordinadas. Singapur cree que es crucial que los debates sobre estas cuestiones, incluidas las leyes, reglas y normas relativas al comportamiento responsable de los Estados, sigan teniendo lugar en las Naciones Unidas, que es el único foro universal, inclusivo y multilateral donde todos los Estados tienen la misma voz.

Singapur participó en el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional para el periodo de 2019 a 2021 y en el 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, establecido en virtud de la resolución 73/27 de la Asamblea General. Participamos activamente y apoyamos los esfuerzos de la Presidencia para crear un grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso 2021-2025 para avanzar en los debates sobre las cibernormas internacionales y el marco acordado para el comportamiento responsable de los Estados en el ciberespacio. Seguimos comprometidos a contribuir de forma constructiva al proceso del grupo de trabajo para seguir reforzando la cooperación internacional y avanzar en el comportamiento responsable de los Estados en el ciberespacio. En su calidad de Copresidente, junto con Estonia, del Grupo de Amigos sobre Gobernanza Electrónica y Ciberseguridad, Singapur seguirá utilizando esta plataforma para concienciar sobre los desafíos del ciberespacio, compartir las mejores prácticas y promover el fomento de la capacidad en las Naciones Unidas.

Reglas, normas y principios de comportamiento responsable de los Estados

Singapur cree que es necesario realizar esfuerzos adicionales para promover el conocimiento de las normas voluntarias y no vinculantes existentes sobre el comportamiento responsable de los Estados y para apoyar su aplicación. Singapur también apoya la elaboración de dichas normas cuando sea necesario. Por ejemplo, las infraestructuras críticas de información transfronterizas que prestan servicios a través de varios Estados, cuya protección es responsabilidad compartida de todos los Estados miembros, podrían considerarse una categoría especial de dichas infraestructuras críticas y deberían incluirse en el conjunto de normas existentes, ya que las amenazas de la tecnología de la información y las comunicaciones (TIC) a dichas infraestructuras podrían tener efectos desestabilizadores a nivel regional y mundial[3].

Las organizaciones regionales pueden desempeñar un papel importante en el apoyo a la aplicación del marco normativo existente. La Asociación de Naciones de Asia Sudoriental (ASEAN) ha suscrito en principio las 11 normas voluntarias y no

[3] La infraestructura de información crítica transfronteriza es una infraestructura de información crítica que pertenece a empresas privadas y que opera a través de las fronteras nacionales, pero que no está bajo la jurisdicción de ningún Estado.

vinculantes sobre el comportamiento responsable de los Estados en el uso de las TIC y, hasta la fecha, sigue siendo la única organización regional que ha adoptado estas normas. En la sexta Conferencia Ministerial de la ASEAN sobre Ciberseguridad, celebrada en 2021, los participantes debatieron los avances del plan de acción regional a largo plazo de la ASEAN sobre la aplicación de normas de comportamiento estatal responsable en el ciberespacio, que pretende garantizar la aplicación efectiva y práctica de estas normas, incluso en los ámbitos de la cooperación entre los equipos de respuesta a emergencias informáticas, la protección de infraestructuras de información críticas y la asistencia mutua en materia de ciberseguridad. El plan de acción regional fue aprobado en el segundo Comité de Coordinación de la Ciberseguridad de la ASEAN en noviembre de 2021 y sigue siendo un documento vivo para su posterior revisión. La estrategia de cooperación en materia de ciberseguridad de la ASEAN para el periodo 2021-2025 actualizó la estrategia de cooperación en materia de ciberseguridad de la ASEAN para crear un ciberespacio más seguro y protegido en la región de la ASEAN. La ASEAN ha acordado establecer un equipo regional de respuesta a emergencias informáticas, que contendrá el mecanismo de intercambio de información del equipo de respuesta a emergencias informáticas de la ASEAN, para reforzar la respuesta de la Asociación a los incidentes de ciberseguridad. A través del directorio de puntos de contacto del Foro Regional de la ASEAN sobre la seguridad de las TIC y su uso, los miembros del Foro pueden ponerse en contacto con sus homólogos en caso de ciberincidentes.

Creación de capacidad

Singapur cree que la creación de capacidades es un pilar esencial del marco normativo acordado, en la medida en que es importante garantizar que todos los Estados tengan la capacidad de aplicar el marco normativo y sus obligaciones en virtud del derecho internacional. En este sentido, Singapur se compromete a compartir su experiencia y sus conocimientos con otros Estados Miembros de las Naciones Unidas, especialmente con los pequeños países en desarrollo, a nivel regional y mundial.

Para apoyar la creación de capacidades a nivel regional (ASEAN), Singapur estableció el Programa de Capacidad Cibernética de la ASEAN en 2016 para apoyar la creación de capacidades en los países de la ASEAN en materia de ciberpolítica, así como en cuestiones operativas y técnicas. A raíz de los comentarios positivos de los socios y participantes internacionales sobre el Programa, Singapur anunció la creación del Centro de Excelencia de Ciberseguridad ASEAN-Singapur en octubre de 2019, con un compromiso de 30 millones de dólares durante cinco años hasta 2023, para llevar a cabo programas de formación en ciberseguridad para altos funcionarios políticos y técnicos de la ASEAN. El campus del Centro se inauguró oficialmente en octubre de 2021 durante la Semana Cibernética Internacional de Singapur. Hasta la fecha, el Centro ha impartido más de 30 programas a los que han asistido más de 1.250 altos funcionarios de la ASEAN y de otros países, y ha colaborado con más de 40 socios de gobiernos, el sector privado, el mundo académico y organizaciones no gubernamentales. A pesar de las restricciones a los viajes derivadas de la pandemia de enfermedad por coronavirus (COVID-19), el Centro siguió impartiendo programas de capacitación en línea y ha organizado 21 programas virtuales de creación de capacidades desde mayo de 2020.

A nivel mundial, Singapur trabaja en colaboración con la Oficina de Asuntos de Desarme en las siguientes iniciativas:

a) En el marco del Programa Cibernético de las Naciones Unidas-Singapur, Singapur está elaborando una lista de verificación de la aplicación de las normas mediante una serie de talleres en varias regiones, en colaboración con la Oficina de

Asuntos de Desarme. La lista de control adoptará la forma de una guía que establece un conjunto de medidas que los países en desarrollo pueden adoptar para aplicar las 11 normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados. Singapur celebró en marzo de 2022 el primer taller sobre la aplicación de las normas para elaborar la lista de comprobación con los Estados miembros de la ASEAN, que se centró en la aplicación de las normas sobre la protección de las infraestructuras críticas, la notificación de vulnerabilidades y la protección de los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de ciberseguridad;

b) A finales de 2022, la Oficina de Asuntos de Desarme y Singapur organizarán conjuntamente la Beca Cibernética Naciones Unidas-Singapur, un programa diseñado para dotar a los altos funcionarios de los Estados Miembros de las Naciones Unidas de los conocimientos interdisciplinarios necesarios para supervisar eficazmente la política, la estrategia y las operaciones nacionales de ciberseguridad y seguridad digital.

Medidas de fomento de la confianza

Singapur también opina que la comunidad internacional debería realizar más esfuerzos para desarrollar medidas de fomento de la confianza en apoyo del marco normativo acordado, dado que dichas medidas tienen el potencial de reducir el riesgo de que se produzcan malentendidos, así como de prevenir y desescalar los conflictos en el ciberespacio. En este sentido, Singapur apoya la creación de un directorio mundial de puntos de contacto nacionales a nivel operativo o técnico, tal y como recomienda el 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. En el segundo semestre de 2022, Singapur también llevará a cabo el primero de una serie de simulaciones para los puntos de contacto cibernéticos nacionales en colaboración con el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR). Los ejercicios (a) ofrecerán a todos los Estados miembros de las Naciones Unidas la oportunidad de participar en un ciberejercicio sustantivo, independientemente de su capacidad técnica actual y/o de su estatus de afiliación a una organización regional; (b) mejorar las capacidades de los puntos de contacto cibernéticos nacionales para responder a incidentes y cibercrisis del mundo real; y (c) demostrar la eficacia y el valor del directorio mundial de puntos de contacto propuesto. Este tipo de ejercicios se han organizado anteriormente a nivel regional entre equipos de respuesta a emergencias informáticas, pero no han estado abiertos a todos los Estados miembros de las Naciones Unidas interesados, especialmente a los que están fuera de las redes regionales de equipos de respuesta a emergencias informáticas establecidas. Para ello, el programa de simulaciones de Singapur será el primer ejercicio abierto a todos los Estados miembros.

Esfuerzos a nivel nacional

A nivel nacional, Singapur ha seguido reforzando la ciberseguridad de sus sistemas y redes en tres frentes, a saber, la construcción de una infraestructura resistente, la habilitación de un ciberespacio más seguro y el desarrollo de un vibrante ecosistema de ciberseguridad.

Construir una infraestructura resiliente

Las entidades que poseen y operan nuestra infraestructura digital principal tienen que cumplir un código de prácticas de ciberseguridad, que detalla las medidas de ciberhigiene que deben practicar dichas entidades, como mantener los sistemas y el software actualizados, mantener copias de seguridad actualizadas de los datos clave

y detectar rápidamente las ciberintrusiones. También se emiten alertas y avisos cuando es necesario para complementar el código de buenas prácticas y hacer frente a las amenazas en evolución (por ejemplo, el programa malicioso secuestrador). Además, la Agencia de Seguridad Cibernética de Singapur lanzó el Plan Maestro de Ciberseguridad de Tecnología Operativa en 2019 como parte de nuestros esfuerzos para mejorar la seguridad y la resiliencia de los sectores de infraestructura de información crítica de Singapur en la prestación de servicios esenciales. El Plan Maestro tiene como objetivo mejorar la respuesta intersectorial para mitigar las ciberamenazas en el entorno de la tecnología operativa y fortalecer las asociaciones con la industria y las partes interesadas esbozando iniciativas clave que abarcan las esferas de las personas, los procesos y la tecnología para mejorar las capacidades de los propietarios de nuestra infraestructura de información crítica y de las organizaciones que manejan sistemas de tecnología operacional. La Agencia también lanzó el marco de competencias básicas de la tecnología operativa, que las empresas pueden aprovechar para establecer procesos, estructuras o puestos de trabajo para gestionar la ciberseguridad de la tecnología operativa en sus organizaciones. En 2022, la Agencia pondrá en marcha un programa de cadena de suministro de infraestructuras de información críticas, en el que participarán partes interesadas como organismos públicos, propietarios de infraestructuras de información críticas y sus proveedores. El programa proporcionará procesos recomendados y prácticas sólidas para que todas las partes interesadas gestionen los riesgos en materia de ciberseguridad en la cadena de suministro.

Un ciberespacio más seguro

Como parte de nuestros esfuerzos para elevar la postura nacional de ciberseguridad en Singapur, la Agencia de Seguridad Cibernética lanzó el Plan Maestro de Ciberespacio más seguro en 2020 para: a) asegurar la infraestructura digital central de Singapur; b) salvaguardar nuestras actividades en el ciberespacio; y c) empoderar a nuestra población familiarizada con las cuestiones cibernéticas. El Plan Maestro esboza 11 iniciativas destinadas a aumentar la adopción de la seguridad por diseño entre las empresas y organizaciones, así como a mejorar la concienciación sobre la ciberseguridad y las buenas prácticas de ciberhigiene entre los usuarios finales. Todas las empresas y organizaciones tienen un papel que desempeñar en la protección de nuestras actividades en el ciberespacio en general. Para facilitarlo, la Agencia ha puesto en marcha una serie de planes para sensibilizar a las partes interesadas en materia de ciberseguridad, como los kits de herramientas de ciberseguridad dirigidos a las diferentes partes interesadas de las empresas. Esto se complementa con la certificación de ciberseguridad para las empresas en forma de las marcas Cyber Trust y Cyber Essentials para reconocer a las empresas con medidas y prácticas de ciberseguridad completas.

La Agencia de Ciberseguridad ha emitido avisos públicos para orientar a las empresas y al público en general sobre la gestión y la navegación de las vulnerabilidades y amenazas relacionadas con la ciberseguridad cuando estas surjan. Por ejemplo, la Agencia emitió un aviso público sobre la reciente vulnerabilidad de Log4Shell y trabajó con asociaciones y cámaras comerciales para informar a las empresas de Singapur sobre cómo abordar la vulnerabilidad y asegurar sus sistemas. Además, la Agencia tiene avisos permanentes sobre la ciberdelincuencia, como un aviso público que desaconseja a las víctimas el pago de rescates a los autores de programas maliciosos secuestradores.

La proliferación de la Internet de los objetos conlleva crecientes riesgos de ciberseguridad, dada su amplia conectividad y la falta de provisión de ciberseguridad. La Agencia de Ciberseguridad ha aprovechado las normas técnicas para elevar la ciberhigiene y ofrecer garantías sobre los productos y servicios. En 2020, la Agencia

puso en marcha el Plan de Etiquetado de Ciberseguridad para los dispositivos de consumo del Internet de los objetos. Ya hay más de 150 productos etiquetados en el mercado. Singapur también es un firme defensor de las normas internacionales basadas en reglas y es una nación que autoriza certificados en el marco del acuerdo de reconocimiento de criterios comunes[4]. Las normas internacionales ayudarán a elevar la ciberhigiene, asegurar el ciberespacio de forma colaborativa y reducir las barreras al comercio transfronterizo. Singapur espera trabajar con socios de ideas afines para desarrollar un marco de etiquetado universal para la seguridad del Internet de los objetos de los consumidores con el fin de armonizar las normas internacionales establecidas y los requisitos de etiquetado, así como para facilitar el reconocimiento mutuo de dichas normas. Esto serviría para minimizar la fragmentación de las normas, erradicar la duplicación de análisis entre países, reducir el coste del cumplimiento de las normativas nacionales y facilitar el acceso al mercado de los desarrolladores.

Desarrollo de un ecosistema de ciberseguridad dinámico

Singapur reconoce que el fortalecimiento de la ciberseguridad implica la construcción del ecosistema cibernético y el fomento de la innovación en la industria. Dada la rápida evolución del panorama de las ciberamenazas, las empresas de ciberseguridad deben innovar constantemente e invertir en nuevas soluciones para mantenerse a la vanguardia. La Agencia de Ciberseguridad apoya la innovación liderada por la industria en materia de ciberseguridad a través de la Convocatoria de Innovación de la Industria de la Ciberseguridad. Esto anima a las empresas de ciberseguridad a desarrollar soluciones innovadoras para satisfacer las necesidades de ciberseguridad de los principales usuarios finales locales (por ejemplo, las entidades que poseen y operan la infraestructura digital básica, y el sector comercial), así como a estimular la demanda en la industria de la ciberseguridad del país. También existe una creciente necesidad de establecer un grupo de personas con talento que puedan asumir funciones de liderazgo en materia de ciberseguridad en las organizaciones. La Agencia ha colaborado con organismos gubernamentales, asociaciones, asociados de la industria y el mundo académico de Singapur para ampliar y desarrollar la fuerza de trabajo en el campo de la ciberseguridad. La iniciativa SG Cyber Talent tiene como objetivo atraer y educar a los entusiastas con talento de la ciberseguridad desde una edad temprana y ayudar a los profesionales de la ciberseguridad a profundizar sus conocimientos. Su meta es llegar a un mínimo de 20.000 personas en un período de tres años para reforzar la cantera de talentos en ciberseguridad en Singapur.

Türkiye

[Original: inglés]
[31 de mayo de 2022]

De acuerdo con las evaluaciones y recomendaciones contenidas en el informe 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 y los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, a continuación se presentan las opiniones y evaluaciones de Türkiye sobre los esfuerzos realizados a nivel nacional para reforzar la seguridad de la información y promover la cooperación internacional en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional, así como el índice de los conceptos mencionados en los informes correspondientes.

[4] Véase www.commoncriteriaportal.org.

Como se destaca en los informes mencionados, nunca ha sido tan evidente el imperativo de construir y mantener la paz, la seguridad, la cooperación y la confianza internacionales en el entorno de las tecnologías de la información y las comunicaciones (TIC). Especialmente debido a la difusión de las tecnologías digitales y a su carácter transfronterizo, la seguridad de las TIC se ha convertido en uno de los elementos primordiales de la defensa nacional y de la seguridad internacional, ya que las ciberamenazas y los delitos se diversifican y amplían. Por ello, los Estados miembros están realizando intensos esfuerzos para crear la infraestructura técnica, la capacidad institucional y el capital humano necesarios en el ámbito de la seguridad nacional. Para prevenir de forma proactiva los posibles riesgos para la seguridad nacional de Türkiye, se están planificando y emprendiendo acciones necesarias como el desarrollo de tecnologías relacionadas con la ciberseguridad y la privacidad de los datos, la resolución de las carencias en cuanto a la disponibilidad de recursos humanos cualificados, la finalización de la reestructuración institucional, la actualización de la infraestructura jurídica y la garantía del cumplimiento de las tecnologías en evolución. Además, es necesario cooperar, especialmente a nivel internacional, para combatir la ciberdelincuencia. En este sentido, el objetivo es seguir desarrollando el intercambio de conocimientos e información y la cooperación internacional para detectar el origen de la ciberdelincuencia y los delincuentes implicados de la manera más eficaz.

Türkiye centra su labor en la adopción de las medidas necesarias para mejorar la ciberseguridad nacional. El Ministerio de Transporte e Infraestructura es el organismo responsable de formular políticas y elaborar estrategias y planes de acción de ciberseguridad nacional en Türkiye. En este contexto, se publicaron y aplicaron la estrategia nacional de ciberseguridad, el plan de acción 2013-2014 y la estrategia y el plan de acción nacionales de ciberseguridad 2016-2019. Türkiye ha desarrollado la estrategia nacional de ciberseguridad y el plan de acción para el periodo 2020-2023 con la participación de todas las partes interesadas en grupos de estudio bajo la coordinación del Ministerio.

La estrategia y el plan de acción nacionales de ciberseguridad para el periodo 2020-2023 se publicaron en el Boletín Oficial el 29 de diciembre e incluye los objetivos estratégicos principales siguientes:

- Proteger las infraestructuras críticas y aumentar la resiliencia
- Fomento de la capacidad nacional
- Red de ciberseguridad orgánica
- Seguridad de las tecnologías de nueva generación
- Lucha contra la ciberdelincuencia
- Desarrollo y fomento de las tecnologías internas y nacionales
- Integración de la ciberseguridad en la seguridad nacional
- Mejora de la cooperación internacional.

El Ministerio de Transportes e Infraestructuras lleva a cabo el seguimiento y la medición relacionados con el plan de acción sobre la base de los pasos de implementación determinados, las actividades que están siendo implementadas por las instituciones y organizaciones responsables, y los criterios de medición.

Al mismo tiempo, el equipo nacional de respuesta a emergencias informáticas de Türkiye, que se encuentra dentro de la Autoridad de Tecnologías de la Información y la Comunicación, ha estado coordinando la respuesta a los ciberincidentes del país desde 2013. Además de la detección de ciberamenazas y la respuesta a

ciberincidentes, antes, durante y después de los incidentes, el equipo garantiza la aplicación de medidas preventivas contra las ciberamenazas y la disuasión cibernética.

Las principales áreas de interés en materia de ciberseguridad del equipo nacional de respuesta a emergencias informáticas son las siguientes

- Creación de cibercapacidades
- Medidas tecnológicas
- Recopilación y difusión de información sobre amenazas
- Protección de las infraestructuras críticas.

En el contexto de la mejora de la ciberseguridad nacional, también se han creado desde 2013 14 equipos sectoriales de respuesta a emergencias informáticas para sectores e infraestructuras críticas (como la energía, la sanidad, la banca y las finanzas, la gestión hídrica, las comunicaciones electrónicas y los servicios públicos críticos) y más de 2.000 equipos institucionales de respuesta a emergencias informáticas. Todos los equipos trabajan 24 horas al día, siete días a la semana, bajo la coordinación del equipo nacional, para mitigar los ciberriesgos y combatir las ciberamenazas. El equipo nacional utiliza herramientas de detección y prevención para la supervisión, y herramientas de notificación para compartir información con las partes pertinentes. Ha desarrollado la plataforma de comunicación para todos los Equipos de Respuesta a Emergencias Informáticas de Türkiye con el fin de distribuir alarmas, avisos y notificaciones de seguridad, lo que proporciona un canal de comunicación eficaz y seguro.

El equipo nacional organiza y apoya cursos de capacitación, campamentos de verano y concursos sobre ciberseguridad abiertos a varias comunidades. Además, imparte capacitación a los Equipos de Respuesta a Emergencias Informáticas sobre temas como análisis de programas maliciosos y análisis de registros. Hasta abril de 2022, más de 5.000 personas habían recibido formación en diferentes ámbitos de la ciberseguridad por parte del equipo nacional.

El equipo nacional ha sido aceptado en el programa Common Vulnerabilities and Exposures (CVE) de la MITRE Corporation y, en este contexto, asigna números CVE para las vulnerabilidades del software, el hardware o los productos de terceros y proporciona coordinación de procesos en la gestión de vulnerabilidades.

Además, la Academia BTK, el centro de formación de la Autoridad de las Tecnologías de la Información y la Comunicación, que se creó en 2017, imparte formación en línea abierta al público sobre ciberseguridad y otras áreas relacionadas con el fin de contribuir a aumentar los conocimientos técnicos dentro de los recursos humanos de Türkiye. El contenido de la formación está disponible en el portal oficial de la Academia en Internet (www.btkakademi.gov.tr/portal).

Varias organizaciones turcas, instituciones, universidades, organizaciones no gubernamentales y entidades del sector privado también organizan seminarios, conferencias y formación en todo el país sobre temas relacionados, como la ciberseguridad y la protección de infraestructuras críticas.

El Día de Internet Segura, que se organiza anualmente, forma parte de las actividades de concienciación de la Autoridad de las Tecnologías de la Información y la Comunicación, cuyo principal objetivo es el uso consciente y seguro de Internet. En el portal oficial de la web más segura (www.guvenlinet.org.tr) hay un teléfono de asistencia para Internet y un sitio web seguro en el que las familias pueden encontrar consejos sobre el uso eficiente de la red.

Además, se imparten cursos y seminarios presenciales y en línea para alumnos, profesores y padres sobre el uso consciente y seguro de Internet. Adicionalmente, se ha llegado a muchos estudiantes realizando visitas escolares con el Camión de Internet Segura, que sirve para que los niños y jóvenes de todo el país interactúen directamente con las nuevas tecnologías y utilicen correctamente la tecnología e Internet, y para concienciar sobre este tema.

Türkiye también toma medidas para contrarrestar los crecientes riesgos de seguridad digital para garantizar la ciberseguridad y ha tomado medidas durante la pandemia de enfermedad por coronavirus (COVID-19).

Los programas maliciosos, los ataques de phishing y otras ciberamenazas que aprovechan las tendencias de la pandemia de COVID-19 son analizados por el Equipo de Respuesta a Emergencias Informáticas, que funciona las 24 horas del día, los siete días de la semana. A través de los centros de mando y control, se determinan y previenen los vínculos malintencionados de estas ciberamenazas para proteger la infraestructura crítica y a los ciudadanos. Dentro de este ámbito, se preparan informes de ciberinteligencia que se comparten con las partes pertinentes. También se han elaborado y publicado varias directrices, sobre los siguientes temas, entre otros:

- Principios de seguridad para las conexiones a distancia
- Proteger a los usuarios de los ataques de phishing
- Las aplicaciones falsas relacionadas con la COVID-19
- Principios de seguridad para la configuración y el uso de software de videoconferencia y reuniones.

Además, las normas profesionales nacionales para el personal de ciberseguridad (nivel 5) entraron en vigor tras su publicación en el Boletín Oficial.

Türkiye ha asumido papeles importantes en muchas organizaciones, ya sea como miembro fundador o contribuyendo a los esfuerzos de cooperación en materia de ciberseguridad y seguridad de la información. En este contexto, Türkiye da la máxima importancia al intercambio de información con diferentes países y organizaciones. Türkiye es miembro de la Unión Internacional de Telecomunicaciones, y el Equipo Nacional de Respuesta a Emergencias Informáticas es miembro del Forum of Incident Response and Security Teams, de Introductores de Confianza, de la Plataforma Multinacional de Intercambio de Información sobre Programa Malicioso de la Organización del Tratado del Atlántico Norte (OTAN), de la Alianza de Ciberseguridad para el Progreso Mutuo y del equipo de respuesta a emergencias informáticas de la Organización de Cooperación Islámica. Türkiye también participa en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN como país patrocinador desde noviembre de 2015. Además, hay esfuerzos en curso relacionados con la cooperación bilateral y multilateral en materia de ciberseguridad, como los memorandos de entendimiento firmados con muchos países. Asimismo, Türkiye apoya la participación activa y la contribución a los estudios de organizaciones internacionales como las Naciones Unidas, la OTAN, la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización de Cooperación y Desarrollo Económicos (OCDE), el Grupo de los 20, la Organización de los Estados Túrquicos, la Organización de Cooperación Económica, la Organización de Cooperación Económica del Grupo de los Ocho Países en Desarrollo y el Centro Regional de Asistencia para la Verificación y Aplicación de Medidas de Control de Armamentos-Centro para la Cooperación en materia de Seguridad.

Los ejercicios de ciberseguridad son otra actividad importante para la cooperación y la preparación. Este tipo de ejercicios a nivel nacional e internacional contribuyen a reforzar el ciberespacio y a poner a prueba las medidas a tomar contra

posibles ciberamenazas. Desde 2011, se han llevado a cabo en Türkiye cinco ejercicios de ciberseguridad nacionales y dos internacionales. Recientemente, los días 12 y 13 de octubre de 2021 se celebró el ejercicio nacional Cyber Shield 2021 en colaboración con el Ministerio de Transportes e Infraestructuras y la Autoridad de Tecnologías de la Información y la Comunicación, con la participación de instituciones y organizaciones públicas. Además, el ejercicio internacional Cyber Shield 2019 fue organizado conjuntamente por el Ministerio y la Autoridad el 19 de diciembre de 2019 en Ankara. El ejercicio contó con el apoyo de la UIT y la Alianza de Ciberseguridad para el Progreso Mutuo. Igualmente, Türkiye sigue participando y contribuyendo a varios ejercicios internacionales de ciberseguridad, como el Locked Shields de la OTAN, la Coalición Cibernética de la OTAN y el Ejercicio de Gestión de Crisis de la OTAN. Adicionalmente a los demás estudios de creación de capacidad y orientación, los ejercicios internacionales de ciberseguridad siguen siendo esenciales para aumentar los niveles de preparación y crear capacidad de respuesta a los ciberincidentes en todo el mundo.

Otra institución importante en el ámbito de las políticas nacionales de TIC es la Oficina de Transformación Digital de la Presidencia de Türkiye.

Uno de los estudios más importantes y destacados realizados por la Oficina de Transformación Digital es la publicación de la Guía de Seguridad de la Información y las Comunicaciones el 24 de julio de 2020. La Guía es el principal documento nacional de referencia publicado en este ámbito. Desempeña un papel importante en el fortalecimiento de las capacidades de ciberdefensa de las instituciones públicas y de los proveedores de servicios de infraestructura crítica.

Se espera que las instituciones públicas y los proveedores de servicios de infraestructura crítica completen sus actividades de cumplimiento en el período especificado en la Guía, y deben realizar auditorías al menos una vez al año. Las políticas y procedimientos de auditoría que deben llevar a cabo las instituciones al respecto están documentadas en la Guía de Auditoría de Seguridad de la Información y las Comunicaciones publicada por la Oficina de Transformación Digital.

Además, se inauguró el Centro Nacional de Bancos de Pruebas de Infraestructuras Críticas, que alberga estudios para garantizar la seguridad de las infraestructuras de distribución de electricidad y gestión del agua, con la colaboración de las partes relacionadas en Türkiye. El Centro, en el que se modelan los sistemas de gestión de la energía y el agua, está diseñado para presentar un entorno de trabajo con el fin de buscar y desarrollar soluciones de protección y prevención relacionadas con la seguridad de la infraestructura crítica y contribuir al ecosistema de la ciberseguridad.

El desarrollo de proyectos para mejorar la seguridad de la información y la ciberseguridad es una de las principales responsabilidades de la Oficina de Transformación Digital, tal como se define en los artículos incorporados por el Decreto Presidencial núm. 48 publicado en la Gaceta Oficial núm. 30928, de fecha 24 de octubre de 2019, al Decreto Presidencial de Organización núm. 1, publicado en la Gaceta Oficial núm. 30474, de fecha 10 de julio de 2018.

En este contexto, se han llevado a cabo varios proyectos relacionados con la información y la ciberseguridad, como el Concurso de Ciberinteligencia y el concurso HackZeugma Capture the Flag:

- El Concurso de Ciberinteligencia forma parte de las actividades de formación y sensibilización destinadas a aumentar el número de personas con conocimientos de ciberseguridad; ha demostrado ser muy eficaz en este sentido. La Oficina de Transformación Digital organizó el segundo Concurso de Ciberinteligencia dentro de las actividades del mes de la ciberconciencia en 2021

- El concurso HackZeugma Capture the Flag fue organizado por la Oficina de Transformación Digital en el marco del Festival Aeroespacial y Tecnológico Teknofest 2020. HackZeugma es una competición que abre sus puertas a miles de hackers de todo el mundo para que puedan demostrar su talento. El concurso se prepara prestando especial atención a la seguridad de los sistemas tecnológicos operativos.

Además, se puso en marcha el proyecto "Un millón de empleos" para crear una mano de obra cualificada en el ámbito de las tecnologías de la información y aumentar el empleo reuniendo a la mano de obra formada con los empresarios. Las nuevas características del proyecto, que permiten a los empleadores escanear los currículos registrándose de forma gratuita y sin condiciones, están disponibles. El proyecto, que depende del Ministerio de Hacienda y Finanzas, tiene como objetivo preparar a un millón de personas para el empleo en el ámbito de las tecnologías de la información para el año 2023 y se lleva a cabo en el ámbito de los objetivos del "Movimiento Tecnológico Nacional" para lograr la transformación digital en nuestro país.

El grupo temático de Ciberseguridad de Turquía es una plataforma seguida de cerca y apoyada por la Oficina de Transformación Digital, cuyo objetivo principal es una Türkiye que produzca tecnología en el campo de la ciberseguridad y sea capaz de competir con el mundo, de acuerdo con las misiones de construir un ecosistema nacional de ciberseguridad, desarrollar productos locales y nacionales de ciberseguridad y difundir su uso. Las actividades realizadas por el grupo temático incluyen:

- Establecer un laboratorio de pruebas y análisis que proporcione infraestructura para las pruebas y el desarrollo del sector
- Creación de un laboratorio de certificación
- Creación de la academia de ciberseguridad
- Organizar actividades nacionales e internacionales como conferencias, formación, seminarios, paneles y ferias, y coordinar las solicitudes y suministros de actividades de prácticas
- Apoyar la apertura de programas de formación de grado medio, de grado y de postgrado.

Además de los esfuerzos mencionados, la Institución Turca de Normalización y la Oficina de Transformación Digital han establecido normas industriales como un enfoque para mejorar la ciberseguridad entre los propietarios y operadores de infraestructura crítica. Se han completado los estudios relacionados con las normas 27701, 27011, 27017, 27018, 27019, 27031, 27799, 31000 y 62443 de la Organización Internacional de Normalización/Comisión Electrotécnica Internacional, y la Institución Turca de Normalización ha publicado normas relativas a la infraestructura crítica.

El desarrollo de la cooperación internacional, junto con las actividades nacionales, es de gran importancia dada la naturaleza de la ciberseguridad. Al extenderse el uso de las TIC en un amplio espectro, la relación que establecen estas tecnologías con temas como la paz, la estabilidad y la seguridad internacionales y los derechos y libertades fundamentales está en continuo desarrollo. Esta situación exige esfuerzos para utilizar las TIC con fines pacíficos y para garantizar que los Estados aborden continuamente la estabilidad y la seguridad internacionales. Es evidente que el derecho internacional, las normas y las reglas expresadas en los informes del Grupo de Expertos Gubernamentales y del Grupo de Trabajo y los estudios pertinentes contribuyen a un marco común de comportamiento responsable de los Estados en el uso de las TIC en el contexto de la paz y la seguridad internacionales. Tal y como se

articula en dichos informes, conceptos como el desarrollo de la cooperación internacional, el respeto de los derechos y libertades fundamentales, la protección de las infraestructuras críticas y la prevención del uso malicioso de las TIC mantendrán su importancia en los esfuerzos hacia la estabilidad y la seguridad internacionales en el próximo periodo.

Al mismo tiempo, hay que tener en cuenta la importancia de proteger la soberanía de los Estados en el ciberespacio y la necesidad de desarrollar nuevas normas además de las existentes. La mejora de la colaboración y el apoyo a los mecanismos de intercambio de información y experiencia son vitales para la lucha contra las ciberamenazas y deben tenerse debidamente en cuenta.

Türkiye es consciente de la importancia de la aplicación del derecho internacional, de las normas de comportamiento responsable de los Estados en el ciberespacio y de las medidas de fomento de la confianza, así como de la necesidad de una cooperación internacional eficaz, y adopta resueltamente las medidas necesarias para alcanzar estos objetivos.

Ucrania

[Original: inglés]
[31 de mayo de 2022]

Ucrania ha sido durante mucho tiempo víctima de la continua agresión armada de Rusia y objetivo de ciberataques en su marco, incluso contra la infraestructura crítica de Ucrania. En consecuencia, Ucrania comparte plenamente la justificada preocupación expresada en el quinto párrafo del preámbulo de la resolución 76/19 de la Asamblea General, con la salvedad de que las tecnologías y los medios de información no solo pueden utilizarse potencialmente, sino que ya son una herramienta aplicada activamente en la práctica por el Estado agresor, y no solo contra Ucrania.

La incapacidad confirmada en repetidas ocasiones por parte de Rusia para observar sus obligaciones internacionales pone en duda su voluntad de cumplir también las disposiciones de los párrafos 3 y 6 de la resolución 76/19.

Lo mismo ocurre con el concebido convenio internacional global sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos que Moscú propuso elaborar. Esto se debe a que si las disposiciones diseñadas por Rusia para su borrador, que crean el riesgo de una grave restricción de los derechos y libertades de los ciudadanos, no pasan a la versión final de la convención, esta no será de interés para Moscú.

Esta restricción, que se propone en el proyecto de convenio ruso, es inaceptable para Ucrania y otros Estados democráticos que son parte del Convenio del Consejo de Europa sobre la Ciberdelincuencia de 2001, pero conviene a los regímenes autoritarios, incluidos los de Rusia y Bielorrusia, que no se adhirieron al Convenio.

A pesar de la agresión militar y cibernética de Rusia, Ucrania está reforzando su sistema de ciberseguridad, con la ayuda material y de asesoramiento de los socios occidentales.

El sistema nacional de ciberseguridad establecido por la Estrategia de Ciberseguridad de Ucrania se basa en el Ministerio de Defensa, el Servicio Estatal de Comunicaciones Especiales y Protección de la Información, el Servicio de Seguridad, la Policía Nacional y el Banco Nacional. Garantiza la colaboración entre todos los organismos públicos, las entidades territoriales, las unidades militares, los organismos encargados de hacer cumplir la ley, las instituciones educativas y de

investigación, las agrupaciones civiles, las empresas y las organizaciones, independientemente de su forma de propiedad, que se ocupan de las comunicaciones electrónicas y la seguridad de la información o son propietarias de infraestructuras de información críticas.

Los sujetos que garantizan el sistema nacional de ciberseguridad están familiarizados con las evaluaciones y recomendaciones contenidas en los informes del Grupo de Trabajo de Composición Abierta sobre los Avances en el Ámbito de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y del Grupo de Expertos Gubernamentales sobre el Avance del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional.

El Consejo Nacional de Seguridad y Defensa de Ucrania coordina y controla las actividades de las entidades del sector de la seguridad y la defensa, garantizando la ciberseguridad de Ucrania a través de su órgano de trabajo, el Centro Nacional de Coordinación de la Ciberseguridad.

El Centro tiene una función de supervisión y realiza tareas relacionadas con el análisis del estado de la ciberseguridad nacional y la preparación para combatir las ciberamenazas, así como la previsión y detección de las amenazas potenciales y reales pertinentes.

Habiendo implementado la anterior Estrategia de Ciberseguridad de Ucrania para el período 2016-2020, el Estado pudo formar el núcleo del sistema nacional de ciberseguridad. Ucrania ha aumentado el potencial que permite un mayor desarrollo del sistema sobre la base de la disuasión, la ciberresiliencia y la interacción.

El objetivo de la actual Estrategia de Ciberseguridad de Ucrania, establecida para el periodo 2021-2025, es crear las condiciones para el funcionamiento seguro del ciberespacio y su uso en interés del individuo, la sociedad y el Estado. El documento se basa en los principios de disuasión, ciberresiliencia e interacción.

Los esfuerzos mencionados permitieron a Ucrania identificar la preparación rusa de los ciberataques maliciosos contra la infraestructura ucraniana que coincidieron con la agresión física. A partir del otoño de 2021, vimos el creciente número de ataques de grupos de hackers afiliados a Rusia contra importantes proveedores ucranianos de servicios digitales y de telecomunicaciones. Estos ataques también aumentaron en calidad, volviéndose más específicos y utilizando herramientas más sofisticadas.

Sin embargo, hay que señalar que la mayoría de esos ciberataques no tuvieron éxito. Nuestras partes interesadas, con el apoyo de nuestros socios internacionales, los detectaron y mitigaron.

Ucrania está desarrollando activamente la cooperación en el ciberdominio, principalmente con Estados Unidos, el Reino Unido, Estonia y otros países occidentales asociados, la Unión Europea y la Organización del Tratado del Atlántico Norte (OTAN). Está recibiendo ayuda financiera, así como asesoramiento, a través de cursos de capacitación bilaterales y multinacionales, seminarios y conferencias en el extranjero y en Ucrania, junto con asistencia, hardware y software modernos para hacer frente a las necesidades de ciberseguridad, llevar a cabo una informática forense profesional e investigar la ciberdelincuencia.

Ucrania agradece la reciente declaración de Estados Unidos, el Reino Unido, la Unión Europea y otros países e instituciones que condenan las acciones agresivas de Rusia en el ciberespacio contra Ucrania y otros países.

Desde 2016, el Ministerio de Asuntos Exteriores de Ucrania ha organizado 22 rondas de ciberconsultas bilaterales con 13 países (Japón, Singapur, Malasia, Finlandia, Estados Unidos, Alemania, Reino Unido, Estonia, Países Bajos, Eslovenia, España, Brasil e Israel). Estas consultas con varios Estados estaban previstas para 2022, pero se pospusieron debido a la invasión militar rusa.

En el campo de la ciberdefensa, Ucrania ha estado cooperando estrechamente con el fondo fiduciario de ciberdefensa de la OTAN para mejorar las capacidades técnicas del país para contrarrestar las ciberamenazas y espera cooperar eficazmente con la alianza como país contribuyente del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN.

Ucrania agradecerá a todos los Estados miembros de las Naciones Unidas que puedan ayudar en la ejecución de los siguientes proyectos que se están llevando a cabo de acuerdo con la actual estrategia de ciberseguridad del país para reforzar las capacidades en el ámbito de la ciberseguridad y la ciberdefensa, y para desarrollar la infraestructura y los servicios de tecnología de la información de una red de centros de situación estatales:

- Construir un cibercampo y realizar ciberejercicios a nivel nacional
- Herramientas de inteligencia de ciberamenazas para plataformas tecnológicas
- Centro nacional de respaldo para los recursos de información críticos del Estado
- Sistema nacional de vigilancia de las ciberamenazas
- Plataforma estatal de servicios de ciberseguridad en la nube.

El Ministerio de Asuntos Exteriores está dispuesto a proporcionar información detallada sobre estos proyectos y ayudar a establecer contacto con sus ejecutores.

La experiencia de Ucrania demuestra que, para hacer frente a las ciberamenazas y ciberataques graves y persistentes, es necesario mejorar la colaboración a múltiples niveles: entre las autoridades nacionales, con el sector privado y con los socios internacionales, a fin de crear las capacidades necesarias y responder eficazmente a dichas amenazas.

III. Respuestas recibidas de organizaciones intergubernamentales

Unión Europea

[Original: inglés]
[31 de mayo de 2022]

El ciberespacio, y en particular la Internet mundial y abierta, se ha convertido en uno de los ejes principales de nuestras sociedades. Ofrece una plataforma que impulsa la conectividad y el crecimiento económico. La Unión Europea y sus Estados miembros apoyan un ciberespacio mundial, abierto, estable y seguro, sobre la base del estado de derecho, los derechos humanos, las libertades fundamentales y los valores democráticos que aportan el desarrollo social, económico y político a nivel mundial.

A medida que Internet y las tecnologías de la información y las comunicaciones (TIC) se van integrando en nuestras vidas, nuestra dependencia de estas tecnologías nos hace cada vez más vulnerables a su uso indebido. El ciberespacio se explota cada vez más con fines maliciosos, y la creciente polarización a nivel internacional está dificultando un multilateralismo eficaz. El comportamiento irresponsable de Rusia en

el ciberespacio forma parte integrante de su invasión ilegal e injustificada de Ucrania y es contrario a las expectativas fijadas por todos los Estados miembros de las Naciones Unidas, incluida la Federación de Rusia, sobre las normas acordadas por las Naciones Unidas de comportamiento estatal responsable. Asimismo, los ataques malintencionados dirigidos contra infraestructura crítica constituyen un riesgo global importante. Las restricciones de Internet y en ella, el aumento de las ciberactividades maliciosas, incluido el incremento de las actividades que afectan a la seguridad e integridad de los productos y servicios de las TIC, amenazan un ciberespacio abierto, libre, global, estable y seguro, así como la democracia, el estado de derecho, los derechos humanos y las libertades fundamentales.

La Unión Europea y sus Estados miembros han expresado periódicamente su preocupación por esas actividades malintencionadas, que socavan el orden internacional basado en normas y aumenta el riesgo de conflicto. El uso malintencionado de las TIC socava los beneficios que Internet y las TIC proporcionan a la sociedad en general y muestra la disposición de algunos actores a amenazar la paz, la seguridad y la estabilidad internacionales. Todos los agentes deben abstenerse de realizar actividades irresponsables y desestabilizadoras en el ciberespacio.

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito

El fortalecimiento de la ciberresiliencia mundial es un elemento crucial para mantener la paz y la estabilidad internacionales, al reducir el riesgo de conflicto y servir como medio para hacer frente a los desafíos asociados a la digitalización de nuestras economías y sociedades. La ciberresiliencia mundial reduce la capacidad de los posibles perpetradores de utilizar indebidamente la TIC con fines malintencionados y fortalece la capacidad de los Estados de responder eficazmente a los ciberincidentes y recuperarse de ellos. La Unión Europea y sus Estados miembros apoyan firmemente la visión antes mencionada de un ciberespacio abierto, libre, mundial, estable y seguro, mediante la promoción y aplicación de un marco estratégico inclusivo y multifacético para la prevención de conflictos y la estabilidad en el ciberespacio, en particular mediante la participación bilateral, regional y de múltiples interesados. Como parte de este marco estratégico, la Unión Europea trabaja para fortalecer la resiliencia mundial, impulsar y promover un entendimiento común del orden internacional basado en normas en el ciberespacio, y elaborar y aplicar medidas prácticas de cooperación, incluidas medidas regionales de fomento de la confianza.

La estrategia de ciberseguridad “Un ciberespacio abierto, protegido y seguro” de 2013, así como los documentos de política, instrumentos y estrategias posteriores que se citan a continuación, representan la visión global de la Unión Europea sobre la mejor manera de prevenir y responder a las perturbaciones y los ataques cibernéticos[5]. Su objetivo es promover los valores de la Unión Europea y asegurar que se den las condiciones para que la economía digital crezca. Algunas medidas específicas están destinadas a aumentar la ciberresiliencia de los sistemas de información, reducir la ciberdelincuencia y fortalecer la política internacional de ciberseguridad y ciberdefensa de la Unión Europea.

En febrero de 2015, el Consejo de la Unión Europea subrayó en sus conclusiones del Consejo sobre la ciberdiplomacia la importancia de seguir desarrollando y ejecutando un planteamiento común y global de la Unión Europea para la ciberdiplomacia que promueva los derechos humanos y los valores fundamentales de

[5] Véase la Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones titulada “Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro”.

la Unión Europea, garantice la libertad de expresión, fomente la igualdad de género, impulse el crecimiento económico, luche contra la ciberdelincuencia, contrarreste las amenazas para la ciberseguridad, evite los conflictos y proporcione estabilidad en las relaciones internacionales[6]. La Unión Europea también pide que se refuerce el modelo multisectorial de gobernanza de Internet y que se intensifiquen los esfuerzos de creación de capacidad en terceros países. Además, la Unión Europea reconoce la importancia de colaborar con los principales asociados y las organizaciones internacionales. La Unión Europea también hace hincapié en la aplicación del derecho internacional vigente en el ciberespacio y en el ámbito de la seguridad internacional y en la pertinencia de las normas de comportamiento, así como en la importancia de la gobernanza de Internet como parte integrante del enfoque común y global de la Unión Europea en materia de ciberdiplomacia.

Sobre la base de un examen de la estrategia de ciberseguridad de 2013, la Unión Europea siguió reforzando sus estructuras y capacidades en materia de ciberseguridad de manera coordinada, con la plena cooperación de los Estados miembros y las distintas estructuras de la Unión Europea pertinentes, respetando al mismo tiempo sus competencias y responsabilidades. En la comunicación conjunta de 2017 titulada "Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE" se establecieron la magnitud del reto y la gama de medidas previstas en la Unión Europea, para garantizar que esté mejor preparada para hacer frente a los crecientes desafíos cada vez mayores de la ciberseguridad[7].

La preocupación por los crecientes problemas de ciberseguridad impulsó la elaboración de un marco para una respuesta diplomática conjunta de la Unión Europea a las actividades informáticas malintencionadas: el conjunto de instrumentos de ciberdiplomacia[8]. La capacidad y disposición crecientes de agentes estatales y no estatales de perseguir sus objetivos mediante actividades cibernéticas malintencionadas debería ser motivo de preocupación a nivel mundial. Esas actividades pueden constituir actos ilegales con arreglo al derecho internacional y podrían tener efectos desestabilizadores y en cascada con mayores riesgos de conflicto. La Unión Europea y sus Estados miembros están firmemente decididos a solucionar las controversias internacionales en el ciberespacio por medios pacíficos. Con este fin, el marco para una respuesta diplomática conjunta de la Unión Europea forma parte del planteamiento de la Unión Europea en materia de ciberdiplomacia, que contribuye a la prevención de conflictos, a contrarrestar las amenazas para la ciberseguridad y a una mayor estabilidad en las relaciones internacionales. El marco fomenta la cooperación, facilita la lucha contra las amenazas inmediatas y a largo plazo e influye en el comportamiento de los agentes malintencionados a largo plazo. También proporciona la debida coordinación con los mecanismos de gestión de crisis de la Unión Europea, incluido el Plan director de respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala. La Unión Europea y sus Estados miembros piden a la comunidad internacional que refuerce la cooperación internacional en favor de un ciberespacio abierto, libre, mundial, estable y seguro en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el estado de derecho. La Unión Europea está decidida a proseguir sus esfuerzos por prevenir, desalentar, disuadir y responder a las actividades malintencionadas, y trata de mejorar la cooperación internacional a tal efecto.

[6] 6122/15 Conclusiones del Consejo sobre la Ciberdiplomacia.

[7] Véase la comunicación conjunta al Parlamento Europeo y al Consejo titulada "Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE".

[8] 9916/17, Proyecto de conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la Unión Europea a las actividades cibernéticas malintencionadas ("Caja de herramientas de ciberdiplomacia").

En diciembre de 2020, la Unión Europea describió en mayor detalle su estrategia para una transformación digital cibersegura en un entorno de amenazas complejas[9]. La estrategia de ciberseguridad de la Unión Europea para la década digital tiene como objetivo promover y proteger un ciberespacio abierto, libre, mundial, estable y seguro, basado en los derechos humanos, las libertades fundamentales, la democracia y el estado de derecho. La estrategia contiene propuestas concretas para abordar la resiliencia, prevenir y disuadir las ciberamenazas y responder a ellas, y promover un ciberespacio mundial y abierto. La prevención del uso indebido de las tecnologías, la protección de las infraestructuras críticas y la garantía de la integridad de las cadenas de suministro también permiten que la Unión Europea se adhiera a las normas, reglas y principios de las Naciones Unidas sobre el comportamiento responsable de los Estados.

La política internacional sobre el ciberespacio de la Unión Europea promueve el respeto de los valores fundamentales de la Unión Europea, define normas para un comportamiento responsable y aboga por la aplicación de las leyes internacionales vigentes en el ciberespacio, al tiempo que ayuda a los países no pertenecientes a la Unión Europea a crear capacidad en materia de ciberseguridad y promueve la cooperación internacional en cuestiones cibernéticas. La Unión Europea sigue trabajando con sus asociados internacionales para impulsar y promover un ciberespacio abierto, libre, mundial, estable y seguro, en el que se respete el derecho internacional, en particular la Carta de las Naciones Unidas, y se cumplan las normas, reglas y principios voluntarios y no vinculantes relativos al comportamiento responsable de los Estados. Para avanzar en la paz y la seguridad en el ciberespacio, existe una clara necesidad de aplicar el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio, tal y como acordaron el anterior Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta sobre los Avances en el Ámbito de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, y que la Asamblea General hizo suyo. Junto con 53 Estados miembros de las Naciones Unidas, la Unión Europea propone establecer un programa de acción para promover un comportamiento responsable de los Estados en el ciberespacio.

Basándose en el acervo existente aprobado por unanimidad por la Asamblea General, el programa de acción ofrece un mecanismo permanente, inclusivo y orientado a la acción en las Naciones Unidas para avanzar en la aplicación de los informes de consenso y apoyar a los Estados en sus políticas nacionales de ciberseguridad, en particular mediante programas de creación de capacidades adaptados a las necesidades identificadas por los Estados beneficiarios. También proporciona un mecanismo institucional dentro de las Naciones Unidas para mejorar la cooperación con otras partes interesadas, como el sector privado, el mundo académico y la sociedad civil, sobre sus respectivas responsabilidades para mantener un entorno de las TIC abierto, libre, seguro, estable, accesible y pacífico. El programa de acción funcionaría de forma complementaria y coordinada con otros procesos pertinentes, como el grupo de trabajo de composición abierta sobre la seguridad de y en el uso de las tecnologías de la información y las comunicaciones 2021-2025.

Con el fin de reforzar su capacidad para anticipar, disuadir y responder a las amenazas y desafíos actuales y emergentes, y salvaguardar los intereses de seguridad de la Unión Europea, esta aprobó formalmente la Brújula Estratégica el 21 de marzo

[9] Véase la Comunicación Conjunta al Parlamento Europeo y al Consejo sobre la estrategia de ciberseguridad de la Unión Europea para la década digital y 7290/21 de 22 de marzo de 2021, Conclusiones del Consejo sobre la estrategia de ciberseguridad de la Unión Europea para la década digital.

de 2022[10]. La Brújula ofrece a la Unión Europea un ambicioso plan de acción para reforzar su política de seguridad y defensa de aquí a 2030, que incluye el fortalecimiento del conjunto de herramientas de ciberdiplomacia de la Unión Europea y el desarrollo de la política de ciberdefensa de la Unión Europea para estar mejor preparada y responder a los ciberataques.

La Unión Europea y sus Estados miembros recuerdan la adopción, el 23 de mayo de 2022, de las conclusiones del Consejo de la Unión Europea sobre el desarrollo de la ciberpostura de la Unión. La postura pretende demostrar la determinación de la Unión Europea de dar respuestas inmediatas y a largo plazo a los actores de las amenazas que pretenden negar a la Unión Europea un acceso seguro y abierto al ciberespacio.

Contenido de los conceptos mencionados en el informe del Grupo de Trabajo y en los informes del Grupo de Expertos Gubernamentales

Amenazas actuales y emergentes

La Unión Europea y sus Estados miembros reconocen que el ciberespacio ofrece importantes oportunidades para el crecimiento económico, así como para el desarrollo sostenible e inclusivo. No obstante, las graves amenazas de las TIC señaladas en anteriores informes del Grupo de Expertos Gubernamentales y en el informe del Grupo de Trabajo persisten y presentan retos en continua evolución[11].

La Unión Europea y sus Estados miembros están preocupados por el aumento de los comportamientos malintencionados en el ciberespacio, como el uso indebido de las TIC con fines malintencionados, tanto por parte de agentes estatales como no estatales, así como por el aumento de los robos de propiedad intelectual por medios cibernéticos. Ese comportamiento socava y amenaza el crecimiento económico, así como la integridad, la seguridad y la estabilidad de la comunidad mundial, y puede tener efectos desestabilizadores y en cascada con mayores riesgos de conflicto.

La pandemia de enfermedad por coronavirus (COVID-19) ha demostrado los riesgos y consecuencias de las actividades maliciosas de las TIC. La Unión Europea y sus Estados miembros han observado ciberamenazas y ciberactividades maliciosas dirigidas a operadores esenciales y reconocen la vulnerabilidad de las infraestructuras de información críticas, las infraestructuras que prestan servicios esenciales al público, las infraestructuras técnicas esenciales para la disponibilidad general o la integridad de Internet, y las entidades del sector sanitario y otras entidades críticas de los Estados miembros y sus socios. La Unión Europea y sus Estados miembros están especialmente alarmados por el aumento de las actividades que afectan a la seguridad e integridad de los productos y servicios de las TIC, que podrían tener efectos sistémicos. También en el contexto del comportamiento irresponsable de Rusia en el ciberespacio como parte integrante de su invasión ilegal e injustificada de Ucrania, la Unión Europea y sus Estados miembros han visto el uso de ciberataques con instrumentos destructivos, como los *wipers* para causar averías en el sistema, pero también interrupciones del servicio, intentos de intrusión, desfiguraciones y ataques distribuidos de denegación de servicio dirigidos a Ucrania, con el potencial de extenderse a otros países, en particular los vecinos de Ucrania.

La Unión Europea y sus Estados miembros condenan este comportamiento malicioso en el ciberespacio, incluida la actividad maliciosa de las TIC destinada a explotar las vulnerabilidades, y subrayan su apoyo constante al aumento de la

[10] 7371/22, “Una brújula estratégica para la seguridad y la defensa - Por una Unión Europea que proteja a sus ciudadanos, valores e intereses y contribuya a la paz y la seguridad internacionales”.

[11] A/75/816.

ciberresiliencia mundial. Cualquier intento de obstaculizar la infraestructura crítica es inaceptable y puede poner en peligro la vida de las personas.

La Unión Europea y sus Estados miembros hacen un llamamiento a todos los países para que no permitan a sabiendas que su territorio se utilice para cometer actos ilícitos a nivel internacional en el ciberespacio utilizando las TIC y para que tomen las medidas adecuadas contra los actores que realicen tales actividades desde su territorio, de conformidad con el Derecho internacional y con los informes de consenso de 2010, 2013, 2015 y 2021 de los Grupos de Expertos Gubernamentales y del Grupo de Trabajo en 2021. La Unión Europea y sus Estados miembros insisten de nuevo en que los Estados deben adoptar todas las medidas apropiadas y razonablemente disponibles y viables para detectar, investigar y abordar la situación.

Además, como se reconoce en informes anteriores del Grupo de Expertos Gubernamentales y del Grupo de Trabajo, dado el carácter único de las TIC, el enfoque de la Unión Europea para abordar las cuestiones cibernéticas en el contexto de la seguridad internacional sigue siendo adaptable a los nuevos desarrollos tecnológicos, al tiempo que señala que las normas de comportamiento responsable del Estado en el ciberespacio son neutrales desde el punto de vista tecnológico. Esto es coherente con el concepto y con el reconocimiento por parte de las Naciones Unidas de que el derecho internacional vigente se aplica a nuevas esferas.

La Unión Europea y sus Estados miembros solo pueden apoyar el desarrollo y el uso de tecnologías, sistemas o servicios dependientes de las TIC que respeten plenamente el derecho y las normas internacionales aplicables, en particular la Carta de las Naciones Unidas, y el derecho internacional humanitario y los derechos humanos.

Forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones

La Unión Europea y sus Estados miembros apoyan firmemente un sistema multilateral eficaz, sustentado en un orden internacional basado en normas, que logre hacer frente a los desafíos mundiales presentes y futuros en el ciberespacio.

Un marco de ciberseguridad verdaderamente universal solo puede basarse en el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos. La Unión Europea y sus Estados miembros reiteran la aplicabilidad del derecho internacional vigente a la conducta de los Estados en el ciberespacio, tal y como reconocen los informes del Grupo de Expertos Gubernamentales de 2010, 2013, 2015 y 2021, así como los principios establecidos en el párrafo 71 b) a g) del informe de 2021 y el Grupo de Trabajo.

El derecho internacional, incluido el derecho internacional humanitario, que incorpora los principios de humanidad, distinción, precaución, necesidad militar y proporcionalidad, se aplica a la conducta del Estado en el ciberespacio y es totalmente protector, al establecer límites claros para su legalidad, también en el contexto de un conflicto. La Unión Europea subraya que el derecho internacional humanitario no es un facilitador de conflictos; En cambio, el derecho internacional humanitario define las normas que rigen las operaciones militares para limitar sus efectos y, en particular, para proteger a la población civil.

Además, los derechos humanos y las libertades fundamentales consagrados en los instrumentos internacionales pertinentes deben respetarse y defenderse por igual en línea y fuera de línea. La Unión Europea y sus Estados miembros se congratulan de que estos principios hayan sido también afirmados por el Consejo de Derechos

Humanos y la Asamblea General, así como por el Grupo de Expertos Gubernamentales y el Grupo de Trabajo[12].

Por estas razones, la Unión Europea y sus Estados miembros no piden la creación de nuevos instrumentos jurídicos internacionales para las cuestiones cibernéticas en este momento, haciendo hincapié en que hay que seguir trabajando para aclarar cómo se aplica el derecho internacional al ciberespacio.

La Unión Europea y sus Estados miembros reafirman su apoyo al diálogo y la cooperación permanentes para promover un entendimiento común sobre la aplicación del derecho internacional vigente a la utilización de las TIC por los Estados, así como su apoyo a los esfuerzos por aportar claridad jurídica sobre la forma en que se aplica el derecho internacional vigente, ya que ello contribuirá a mantener la paz, prevenir los conflictos y garantizar la estabilidad mundial.

Seguimos apoyando los esfuerzos en curso para promover la aplicación del derecho internacional vigente en el ciberespacio, en particular en lo que respecta al intercambio de información y las mejores prácticas sobre la aplicación del derecho internacional vigente en el ciberespacio. Nos comprometemos a seguir informando sobre las posiciones nacionales acerca de la forma en que el derecho internacional se aplica al uso de las TIC por los Estados, ya que promueve la transparencia y fomenta el entendimiento mundial sobre los enfoques nacionales, lo cual es fundamental para mantener la paz y la estabilidad a largo plazo y reduce el riesgo de conflicto mediante actos en el ciberespacio. Se debería hacer más hincapié en la concienciación y el desarrollo de capacidades sobre la aplicabilidad del derecho internacional existente como medio para promover la estabilidad y prevenir los conflictos en el ciberespacio.

Normas, reglas y principios de comportamiento responsable de los Estados

La Unión Europea y sus Estados miembros alientan a todos los Estados a que se basen en la labor respaldada reiteradamente por la Asamblea General, en particular en su resolución 76/19, y a que avancen en la aplicación de estas normas acordadas y de las medidas de fomento de la confianza, que desempeñan un papel esencial en la prevención de conflictos.

La Unión Europea y sus Estados miembros se guían y se guiarán en su uso de las TIC por el derecho internacional vigente, así como por la adhesión a las normas, reglas y principios voluntarios y no vinculantes de comportamiento responsable de los Estados y su aplicación en el ciberespacio, tal como se articula en los sucesivos informes del Grupo de Expertos Gubernamentales de 2010, 2013, 2015 y 2021. La continuación de un diálogo inclusivo y constructivo dentro del grupo de trabajo _____ es bienvenida para seguir profundizando en los debates sobre este marco y sobre los retos de seguridad relacionados con el uso de las TIC. Creemos que para avanzar de una forma práctica se debería alentar una mayor cooperación y transparencia para compartir las mejores prácticas, en particular sobre la forma en que se aplican las normas existentes del Grupo de Expertos Gubernamentales, mediante iniciativas y marcos conexos, como las organizaciones e instituciones regionales, con miras a facilitar la sensibilización y aplicar eficazmente las normas acordadas sobre el comportamiento responsable de los Estados.

Medidas de fomento de la confianza

La creación de mecanismos eficaces de cooperación e interacción entre los Estados en el ciberespacio es un componente esencial de la prevención de conflictos. Los foros regionales han demostrado ser una plataforma pertinente para crear un

[12] Véase la resolución 20/8 del Consejo de Derechos Humanos.

espacio para el diálogo y la cooperación entre agentes con preocupaciones e intereses comunes, a fin de abordar eficazmente los problemas desde una perspectiva regional.

La elaboración y aplicación de medidas de fomento de la confianza cibernética, incluidas las medidas de cooperación y transparencia, en la Organización para la Seguridad y la Cooperación en Europa, el Foro Regional de la Asociación de Naciones de Asia Sudoriental, la Organización de los Estados Americanos y otros entornos regionales aumentará la previsibilidad del comportamiento de los Estados y reducirá el riesgo de interpretación errónea, escalada y conflicto que pueden derivarse de incidentes relacionados con las TIC, contribuyendo así a la estabilidad a largo plazo en el ciberespacio.

Cooperación y asistencia internacionales en materia de seguridad y fomento de la capacidad en el ámbito de las tecnologías de la información y las comunicaciones

A fin de prevenir conflictos y reducir las tensiones derivadas del uso indebido de las TIC, la Unión Europea y sus Estados miembros se proponen fortalecer la resiliencia mundial, haciendo especial hincapié en los países en desarrollo, como medio de hacer frente a los retos asociados a la digitalización de las economías y las sociedades, y de reducir la capacidad de los posibles perpetradores de utilizar indebidamente las TIC con fines malintencionados. La resiliencia aumenta la capacidad de los Estados de responder eficazmente a las ciberamenazas y recuperarse de ellas.

La Unión Europea y sus Estados miembros prestan apoyo a una serie de programas e iniciativas a medida para ayudar a los países a desarrollar sus aptitudes y capacidades para hacer frente a los ciberincidentes, así como iniciativas para facilitar el intercambio de mejores prácticas, ya sea mediante la participación directa, los contactos bilaterales o la participación a través de instituciones regionales y multilaterales.

La Unión Europea y sus Estados miembros reconocen que la promoción de una capacidad de protección adecuada y de productos, procesos y servicios digitales más seguros contribuirá a que el ciberespacio sea más seguro y fiable. Reconocemos la responsabilidad de todos los agentes pertinentes de participar en el desarrollo de la capacidad a este respecto y pedimos además una cooperación más estrecha con los principales asociados y organizaciones internacionales para apoyar la creación de capacidad en terceros países. La Unión Europea y sus Estados miembros conceden especial importancia a la mejora de la seguridad y la estabilidad internacionales en el ciberespacio, fomentando y facilitando acciones concretas en relación con el comportamiento responsable de los Estados en el ciberespacio y reforzando la cooperación en materia de fomento de la capacidad cibernética, entre otras cosas con el apoyo de un mecanismo de facilitación en las Naciones Unidas a fin de fomentar programas de fomento de la capacidad adaptados a las necesidades identificadas por los Estados beneficiarios, como el programa de acción, y la determinación de mecanismos que faciliten el compromiso de todas las partes interesadas en la aplicación del marco de comportamiento responsable.