Naciones Unidas A/76/187

Asamblea General

Distr. general
19 de julio de 2021
Español
Original: español/inglés

Septuagésimo sexto período de sesiones
Tema 96 del programa provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/76/150.

21-10045 (S) 160921 170921

I. Introducción

1. El 7 de diciembre de 2020, la Asamblea General aprobó la resolución 75/32, titulada “Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional”, en relación con el tema del programa “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”.

2. En el párrafo 2 de la resolución, la Asamblea General invitó a todos los Estados Miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuraban en los informes del Grupo de Expertos Gubernamentales, siguieran 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 los informes del Grupo de Expertos Gubernamentales.

3. En cumplimiento de esa solicitud, el 18 de febrero de 2021 se envió una nota verbal a todos los Estados Miembros para invitarlos a proporcionar información sobre el tema. A fin de facilitar a los Estados Miembros la presentación de sus opiniones sobre las cuestiones mencionadas, el plazo de presentación se fijó en el 31 de mayo de 2021.

4. Las respuestas recibidas hasta el momento en que se preparó el informe figuran en las secciones II y III *infra*. Las respuestas adicionales recibidas después del 31 de mayo de 2021 se publicarán en el sitio web de la Oficina de Asuntos de Desarme[1] en el idioma original en que se hayan recibido. No se publicarán adiciones.

II. Respuestas recibidas de los Gobiernos

Australia

[Original: inglés]
[31 de mayo de 2021]

Australia acoge con beneplácito la oportunidad, en respuesta a la invitación formulada en la resolución 75/32 de la Asamblea General, de exponer sus opiniones sobre la promoción de un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. Esta presentación se basa en la información proporcionada por Australia en respuesta a las resoluciones 74/28 en 2020, 70/237 en 2016, 68/243 en 2014 y 65/41 en 2011 sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

Estrategia de Participación Internacional en materia de Cibernética y Tecnología Crítica

El 21 de abril de 2021, la Ministra de Relaciones Exteriores, Marise Payne, lanzó la Estrategia de Participación Internacional en materia de Cibernética y Tecnología Crítica, que establece los intereses y objetivos de Australia en el ciberespacio y la tecnología crítica. El objetivo general de Australia es una Australia,

[1] http://www.un.org/disarmament/ict-security.

una región indopacífica y un mundo seguros y prósperos gracias al ciberespacio y la tecnología crítica (www.internationalcybertech.gov.au/).

La Estrategia establece los intereses de Australia en la consecución de este objetivo en todo el espectro de cuestiones relativas al ciberespacio y la tecnología crítica. Esto incluye nuestros principios y valores fundamentales de derechos humanos, estado de derecho, equidad, competencia abierta, seguridad, transparencia, respeto e integridad.

La Estrategia identifica tres pilares principales, a saber, los valores, la seguridad y la prosperidad, que deben guiar la participación internacional de Australia en materia de ciberespacio y tecnología crítica:

a) *Valores.* Australia siempre perseguirá un enfoque del ciberespacio y la tecnología crítica basado en los valores y se opondrá a los esfuerzos por utilizar las tecnologías con el fin de socavar esos valores;

b) *Seguridad.* Australia apoyará en todo momento la paz y la estabilidad internacionales y una tecnología segura, fiable y resiliente.

c) *Prosperidad.* Australia siempre abogará por que el ciberespacio y la tecnología fomenten el crecimiento económico sostenible y el desarrollo para aumentar la prosperidad.

El 6 de agosto de 2020, Australia también publicó *Australia's Cyber Security Strategy 2020* (Estrategia de Ciberseguridad de Australia de 2020) con el fin de lograr un mundo en línea más seguro para los australianos, sus empresas y los servicios esenciales de los que depende Australia (www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf).

Marco del comportamiento responsable de los Estados en el ciberespacio

Ante el progresivo aumento del poder e influencia que ejercen los Estados en el ciberespacio, Australia considera importante que existan normas claras. 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 de 2010 (A/65/201), 2013 (A/68/98) y 2015 (A/70/174) se afirma de manera acumulativa que el derecho internacional vigente es aplicable y esencial para mantener la paz y la estabilidad en el ciberespacio. 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, el derecho internacional, las normas, las medidas de fomento de la confianza y la creación de capacidad constituyen la base de un ciberespacio seguro, estable y próspero, y a menudo se hace referencia a ellos como un marco para un comportamiento responsable de los Estados.

Australia ha participado activamente en dos procesos recientes de las Naciones Unidas en los que se ha estudiado el comportamiento responsable de los Estados en el ciberespacio y que concluyeron en 2021: el sexto Grupo de Expertos Gubernamentales (véase A/76/135) y el Grupo de Trabajo de Composición Abierta (véase A/75/816), que reafirman ese marco y se apoyan en él.

Australia reafirma su compromiso de actuar de conformidad con los informes acumulativos del Grupo de Expertos Gubernamentales de 2010, 2013, 2015 y 2021 (A/65/201, A/68/98 y A/70/174) y el informe del Grupo de Trabajo de Composición Abierta (A/75/816).

Derecho internacional

La posición de Australia sobre cómo se aplica el derecho internacional a la conducta de los Estados en el ciberespacio se presenta en una serie de documentos: *Australia's 2017 International Cyber Engagement Strategy* (Estrategia de Participación Cibernética Internacional de Australia de 2017) (www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy), *2019 International Law Supplement* (Suplemento de Derecho Internacional de 2019) (https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF), los estudios monográficos sobre la aplicación del derecho internacional en el ciberespacio publicados en febrero de 2020 (https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studieson-the-application-of-international-law-incyberspace.pdf), *Australia's International Cyber and Critical Technology Engagement Strategy 2021* (Estrategia de Compromiso Cibernético Internacional y de Tecnología Crítica de Australia de 2021) y la comunicación de Australia sobre el derecho internacional que se adjuntará al informe de 2021 del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional (pendiente de publicación).

Participación de múltiples interesados

Australia reconoce la importancia de la comunidad de múltiples interesados, incluidos la sociedad civil, el sector privado, el mundo académico y la comunidad técnica, a la hora de contribuir a un ciberespacio libre, abierto, seguro, estable, accesible y pacífico.

Para ello, Australia tuvo el placer de copatrocinar la iniciativa LetsTalkCyber (letstalkcyber.org), que proporcionó una plataforma para que múltiples interesados realizaran aportaciones al Grupo de Trabajo de Composición Abierta y colaboraran con él, y para la realización de consultas entre los Estados, la sociedad civil, el sector privado, el mundo académico y la comunidad técnica. Australia también llevó a cabo varias rondas de consultas con múltiples interesados nacionales y solicitó activamente los puntos de vista de la comunidad de múltiples interesados para informar de sus posiciones en los procesos del Grupo de Trabajo de Composición Abierta y del Grupo Gubernamental de Expertos.

Además, Australia creó la Red Quad Tech para apoyar la investigación y promover la colaboración entre los Estados y los académicos y grupos de reflexión asociados de Australia, los Estados Unidos de América, la India y el Japón en cuestiones de cibernética y tecnología crítica. La Red Quad Tech producirá investigaciones y recomendaciones pertinentes para la formulación de políticas, profundizará y reforzará la comprensión por parte del público de los problemas del ciberespacio y la tecnología crítica, y promoverá un diálogo público fundamentado. La Red se inauguró el 9 de febrero con una serie de documentos públicos sobre paz y seguridad internacionales, conectividad y resiliencia regional, derechos humanos y ética, y seguridad nacional (www.internationalcybertech.gov.au/node/139).

Colombia

[Original: español]
[31 de mayo de 2021]

En atención a la resolución 75/32 de las Naciones Unidas, relativa a la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, Colombia se permite comunicar al Secretario General, con base en las evaluaciones y recomendaciones que figuran en los informes

del Grupo de Expertos Gubernamentales, las siguientes opiniones y observaciones sobre:

– Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional.

– El contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales.

Al respecto, cabe aclarar que el presente informe complementa el presentado en el año 2020, haciendo énfasis en los desarrollos llevados a cabo el último año, y principalmente en relación con las recomendaciones extraídas del informe del Grupo de Expertos Gubernamentales de 2015 para el examen por los Estados con miras a promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las tecnologías de la información y las comunicaciones (TIC).

Normas, reglas y principios voluntarios de comportamiento responsable de los Estados

Los Estados, en consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, deberían colaborar en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el uso de las TIC y evitar las prácticas en la esfera de las TIC que se consideran que son perjudiciales o que pueden poner en peligro la paz y la seguridad internacionales.

De igual manera los elementos de apropiación fueron trabajados en la Política Nacional de Confianza y Seguridad Digital (documento 3995/2020 del Consejo Nacional de Política Económica y Social), en donde se señala que uno de los objetivos primordiales es fortalecer las capacidades en seguridad digital de los ciudadanos en los sectores público y privado.

Al respecto, el Gobierno de Colombia, desde el Ministerio de Tecnologías de la Información y las Comunicaciones, el Servicio National de Aprendizaje y el Ministerio de Educación Nacional, ha desarrollado una serie de actividades que se apoyan en la estrategia de apropiación, contemplada en los siguientes programas específicos:

- Por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, en el programa “Hablemos de Gobierno Digital”, desarrollado de 2020 a 2021, se sensibilizó en ciberseguridad digital a la ciudadanía a través de 15 sesiones, llegando a más de 4.000 personas. De igual forma, en 2020 se realizaron tres talleres dirigidos a emprendedores y microempresas y pequeñas y medianas empresas, con la participación de 483 personas, incluyendo 156 mujeres, donde se les capacitó en seguridad digital. Igualmente, se realizaron dos talleres en conceptos específicos del Modelo de Seguridad y Privacidad de la Información.
- En el marco del “Mes de la Seguridad Digital” se realizaron varias actividades, entre las que destacan cuatro talleres sobre temáticas especializadas en la gestión de incidentes con el apoyo de Cisco y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia; dos talleres sobre la importancia de realizar auditorías y la gestión de riesgos en las entidades públicas; dos sesiones de “Hablemos de Gobierno Digital”, sobre el resultado del ejercicio realizado con la Organización de los Estados Americanos (OEA); la primera reunión del Consejo de Innovación en Ciberseguridad realizado en Colombia; y dos charlas denominadas “Recomendaciones para no ser víctima de los ciberdelincuentes” y “Desinformación en las redes con un enfoque jurídico”, dirigidas al público

en general. Para el cierre se realizó, junto con la OEA, el Segundo Consejo de Innovación en Ciberseguridad. Estas actividades sumaron una participación de 1.040 personas, entre funcionarios de entidades públicas y usuario final, con un 45 % de participación de mujeres.

- En el evento de “Colombia 4.0”, en las actividades desarrolladas en el CIO Summit 2020, que vinculó a líderes de tecnología de entidades públicas, se vincularon 490 personas a través de la conferencia “Cómo sobrevivir al COVID-19 y la transformación digital y no ser hackeado en el intento”. Asimismo, se desarrolló el taller “Mejores prácticas para la detección y respuesta de amenazas basadas en el modelo MITRE ATT&CK y XDR”, en el que se calcula que un 40 % de participantes fueron mujeres. En este contexto, se realizaron actividades de sensibilización acerca del Modelo de Seguridad y Privacidad de la Información, en las que participaron aproximadamente 3.196 funcionarios de 1.834 entidades, incluidas 131 del orden nacional y 1.224 del orden territorial.

- En la iniciativa “Talento Digital”, llevada a cabo por el Ministerio de Tecnologías de la Información y las Comunicaciones, se realizó la convocatoria de “Habilidades Digitales - Formación en Ciberseguridad”, cuyos objetivos apuntaron a la selección de personal colombiano para formarlos y capacitarlos en temas de ciberseguridad. Se ofrecieron dos diplomados para la formación en habilidades especializadas: i) un diplomado en ciberseguridad para directivos o gerentes y ii) un diplomado en ciberseguridad para personal técnico.

- Por su parte, el Servicio Nacional de Aprendizaje adelanta los siguientes programas: Seguridad en Redes de Computadores; Gestión y Seguridad de Bases de Datos; Gestión y Seguridad de Bases de Datos; Control de la Seguridad Digital; Programación de *Firmware* en Dispositivos; Introducción a los Sistemas de Gestión de la Seguridad de la Información según la Norma ISO IEC 27001; Aplicación de técnicas de Diagnóstico en Ciberseguridad; y Gestión de la Seguridad Informática.

- El Ministerio de Educación ha adelantado acciones para apropiación relacionadas con la difusión de contenidos (uso de redes sociales, campañas y talleres con entidades públicas y microempresas y pequeñas y medianas empresas). También se han establecido alianzas con el sector privado y cooperación internacional.

- Asimismo se ha trabajado en diplomados, beneficiando a 2.216 docentes, y se ha incorporado la estrategia de seguridad digital en el marco del proyecto Aprender Digital para estudiantes de educación primaria, básica y media, beneficiando a 4.093 estudiantes, incluyendo en el portal “Colombia Aprende”, con más de 30 contenidos.

En lo referente a la recomendación referida a que “los Estados no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC”, el Gobierno de Colombia ha desarrollado las siguientes actividades:

- Como mecanismo de articulación y gobernanza, la Política Nacional de Confianza y Seguridad Digital (documento 3995/2020 del Consejo Nacional de Política Económica y Social) estableció un coordinador nacional, rol que desarrolla la Consejería Presidencial para Asuntos Económicos y Transformación Digital, y el Comité de Seguridad Digital, cuerpo colegiado integrado por los estamentos en materia de seguridad digital y cuyo propósito es estudiar temas específicos de seguridad digital en niveles estratégicos y contando con el encargo de abordar las temáticas de: 1) política y normatividad

para la seguridad digital; 2) protección y defensa de la infraestructura crítica cibernética nacional; 3) gestión de riesgos de seguridad digital; 4) crisis y seguimiento amenazas cibernéticas; 5) protección de datos personales; 6) asuntos internacionales de seguridad digital; y 7) comunicaciones estratégicas para la seguridad digital.

- Estableció un puesto de mando unificado en materia de seguridad digital con el fin de garantizar la seguridad e integridad de la infraestructura tecnológica y sitios web del sector gobierno durante el desarrollo de fechas patrias, así como durante los comicios electorales y otras situaciones coyunturales. Sus objetivos son: i) la ciberseguridad ciudadana y ciberdefensa del Estado; ii) la prevención, anticipación e investigación judicial; iii) la atención de incidentes cibernéticos; iv) la estabilidad del estamento gubernamental e institucional; y v) el fortalecimiento lógico. Se establecieron protocolos de actuación para responder a posibles escenarios de ataque como son el ataque de negación de servicio distribuido de los portales web (DDOS), vulnerabilidades web y noticias falsas.
- Se han realizado actividades en coordinación con el Senado de la República, a través de las cuales se ofreció la capacitación del desarrollo de mejores prácticas para el uso de plataformas virtuales.

En cuanto a las mejores maneras de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines terroristas o delictivos y aplicar otras medidas de cooperación para hacer frente a tales amenazas, el 16 de marzo de 2020 Colombia se adhirió al Convenio sobre la Ciberdelincuencia, adoptado en Budapest en 2001, el cual entró en vigor para nuestro país el 1 de julio de 2020. Actualmente se trabaja en su implementación.

En lo relacionado con las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, Colombia ha tomado medidas adecuadas, a través del fortalecimiento del equipo de respuesta a incidentes de ciberseguridad del Gobierno, en pro de la protección de las instituciones públicas. El proyecto contempla la estructuración de un proceso a través del cual se estima contratar una solución integral para robustecer la prestación de los servicios prestados por el equipo de respuesta a incidentes de ciberseguridad del Gobierno de manera más eficiente a las entidades del Estado, logrando un mayor impacto en todo el territorio, a través de mejoras de la infraestructura de tecnología de la información, física y del talento humano, garantizando un servicio en modalidad 24/7.

Dentro de las iniciativas que se han propuesto, se plantea la elaboración del diagnóstico actual y el plan de mejoramiento continuo de sus propias capacidades operativas, administrativas, humanas, científicas y de infraestructura tecnológica, con el fin de apalancar recursos para el fortalecimiento de dichas entidades en materia de seguridad digital. Igualmente, está el proyecto para el traslado y la optimización del equipo de respuesta a incidentes de ciberseguridad del Gobierno.

Por otro lado, en cuanto a la recomendación referida a que los Estados deberían alentar la divulgación responsable de las vulnerabilidades relacionadas con las TIC y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o infraestructuras dependientes de esas tecnologías, en Colombia se está fomentando la notificación responsable de las vulnerabilidades de las TIC y se están tomando medidas razonables para garantizar la integridad de la cadena de suministro y prevenir la proliferación de herramientas, técnicas o funciones ocultas dañinas de las TIC malintencionadas, en el marco del trabajo con la OEA y la Organización para la Cooperación y el Desarrollo Económicos.

Con el nuevo documento de política pública (documento 3995/2020 del Consejo Nacional de Política Económica y Social) titulado “Política Nacional de Confianza y Seguridad Digital”, se estableció una acción concreta para contar con un modelo para la divulgación periódica de vulnerabilidades en todos los sectores con un alcance definido entre los puntos de contacto de los propietarios y operadores de activos que soportan actividades críticas y las instancias pertinentes del Gobierno nacional. Para el desarrollo de este modelo se involucrarán a las múltiples partes interesadas y se contemplarán experiencias internacionales al respecto.

Respecto a la recomendación referida a que los Estados no deberían realizar ni apoyar de forma deliberada actividades que dañaran los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias cibernéticas o equipos de respuesta a incidentes de seguridad informática) de otro Estado, y que un Estado no debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada, en Colombia se han tomado medidas compatibles con el derecho internacional y las reconocidas en la Carta de Naciones Unidas, teniendo como responsabilidad primordial el garantizar un entorno seguro y pacífico en la esfera de las tecnologías de la información y las comunicaciones.

De igual manera, el Gobierno de Colombia emitió la resolución 500 y la Directiva Presidencial 03 de marzo de 2021, con el fin de establecer los lineamientos y estándares para la estrategia de seguridad digital, y adoptando el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

El Decreto 2106 de 2019, artículo 16, incluyó normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, y señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

A través del Modelo de Seguridad y Privacidad de la Información, como habilitador de la política de Gobierno Digital, el Ministerio de Tecnologías de la Información y las Comunicaciones dispone los lineamientos generales para su implementación, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital, estableciendo los lineamientos y estándares para la estrategia de seguridad digital.

Frente a un posible ataque cibernético, en Colombia se opta por medidas que impliquen la aplicación de la ley, inteligencia y herramientas diplomáticas, teniendo como propósito frenar un ataque y prevenir la destrucción de bienes o la pérdida de vidas, agotando todas las opciones de defensa de la red antes de realizar una operación en el ciberespacio.

El Gobierno de Colombia, a través del desarrollo de la política nacional de seguridad digital, ha orientado sus esfuerzos en tres pilares fundamentales: i) la generación de capacidades para la gestión de los riesgos del entorno digital; ii) el desarrollo de una institucionalidad que apoya la gobernanza; y iii) la evaluación de marcos de trabajo y buenas prácticas internacionales. Para su cumplimiento se plantean las siguientes estrategias:

- Elaborar el diagnóstico actual y el plan de mejoramiento continuo de sus propias capacidades operativas, administrativas, humanas, científicas y de infraestructura tecnológica.
- Definir los lineamientos para la conformación de una red de participación cívica digital que permita a las múltiples partes interesadas interactuar y cooperar

frente a una amenaza cibernética, fortaleciendo y ampliando las capacidades de seguridad digital en Colombia en el marco del derecho internacional.

- Coordinar la elaboración de lineamientos para los planes de mejora en seguridad digital con el fin de fortalecer las capacidades del sistema de seguridad social integral en el manejo, gestión e intercambio de la información, dada la condición de infraestructura crítica cibernética del sistema de seguridad social integral.
- Establecer dentro del modelo nacional de gestión de incidentes, los lineamientos con las condiciones especiales para la gestión de riesgos y el manejo de incidentes en seguridad digital relacionados con el manejo, gestión e intercambio de la información del sistema de seguridad social integral, las cuales deberán integrarse con el procedimiento general de atención a incides establecido por el Comité de Seguridad Digital.
- Coordinar la incorporación de los mecanismos idóneos del caso (técnicos, legales, organizacionales, etc.) que permitan recopilar la evidencia digital necesaria en caso de materialización de algún incidente cibernético dentro del manejo, gestión e intercambio de la información del subsistema de salud del sistema de seguridad social integral.
- Diseñar, estructurar y presentar el proyecto de implementación del equipo de respuesta a incidentes de ciberseguridad del sector de la seguridad social integral.
- Diseñar, estructurar y presentar el proyecto de implementación del equipo de respuesta a incidentes de ciberseguridad del sector inteligencia, con el fin que contribuya en la protección de la seguridad digital nacional.
- Diseñar una propuesta del registro central único de incidentes de seguridad digital a nivel nacional, con el fin de analizar las tipologías de los incidentes y valorar periódicamente la necesidad de priorizar estrategias y recursos para su gestión. Dicho registro central único de incidentes deberá integrar los reportes existentes en la materia realizados por las múltiples partes interesadas procurando simplificar el envío, determinando medios seguros de entrega y garantizando la confidencialidad, conservación y uso adecuado de la información que se intercambie entre partes.

Se procura garantizar los derechos y libertades constitucionales de los ciudadanos en el campo de la obtención y uso de la información, en consonancia con nuestra Constitución Política.

Se han adoptado medidas en la legislación colombiana, necesarias para prever como infracción penal: i) el acceso doloso y sin autorización a todo o parte de un sistema informático; ii) la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos; iii) la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos; y iv) la producción y difusión o transmisión de pornografía infantil.

Se avanza en el desarrollo de una definición clara de la infraestructura crítica nacional e internacional, identificando los sectores cuyos productos o servicios califican como infraestructura crítica y mantener una lista de activos críticos. Estas definiciones se están compartiendo con la comunidad internacional como medida de fomento de la confianza.

Igualmente, se trabaja en el establecimiento de redes de resolución de crisis entre los actores de entidades públicas relevantes que soliciten el apoyo. Para ello, también se proyecta la articulación con la comunidad internacional estableciendo una red de puntos de contacto “a nivel político y técnico”. Al respecto, Colombia ha:

- Proyectado ejercicios de ciberseguridad nacionales e internacionales, para poner a prueba periódicamente su capacidad para comunicarse con otros Estados, así como su capacidad para responder a las solicitudes de asistencia y mitigación (en particular, canales de comunicación, protocolos y procedimientos), mediante ejercicios conjuntos de ciberseguridad.
- Participado en espacios con CyberEX, CyberDrills de la Unión Internacional de Telecomunicaciones y se coordina con el Comando Conjunto Cibernético los ejercicios nacionales de simulacro nacional de crisis.
- Utilizado redes nacionales de resolución de crisis de múltiples partes interesadas preestablecidas y se ha apoyado en la experiencia de mitigación proporcionada por el Estado y los actores no estatales en el evento de una operación cibernética de este tipo, siguiendo las mejores prácticas existentes relativas a la notificación de incidentes en el contexto nacional e internacional.
- Desarrollado ejercicios con agremiaciones. A partir de los ataques que se dieron en medio de las protestas sociales en el ciberespacio mediante amenazas de grupos hacktivistas tanto al Gobierno como a empresas privadas, desde la Federación Colombiana de la Industria del Software y Tecnologías Informáticas han realizado un acercamiento con el gobierno, en nombre de un grupo de empresas para desarrollar soluciones específicas en seguridad digital. A partir de estos acercamientos se han realizado unas reuniones para revisar en qué puntos se podría apoyar al Gobierno, para esto se hizo un levantamiento dentro de las empresas afiliadas frente a capacidades de inteligencia y monitoreo.

Frente a la cooperación internacional en caso de una operación cibernética maliciosa contra la infraestructura crítica, el Gobierno de Colombia ha realizado trabajos de cooperación conjuntos con Estados Unidos.

Medidas de fomento de la confianza de carácter voluntario

En cuanto a la promoción de la cooperación, en particular mediante el establecimiento de centros de coordinación para intercambiar información sobre la utilización malintencionada de las TIC y prestar asistencia en investigaciones, a través del Centro Cibernético Policial de la Dirección de Investigación Criminal y la Organización Internacional de Policía Criminal (INTERPOL), la Policía Nacional, desde tres componentes diferenciales en ciberseguridad (prevención, investigación e informática forense), realiza la articulación con las diferentes entidades que componen el Comité de Seguridad Digital del Gobierno Nacional.

Esto permitió durante los años 2020 y 2021 generar las siguientes actividades: desarrollo de 32 campañas operativas contra el cibercrimen, logrando 219 capturas por delitos informáticos; atención de 14.072 incidentes en ciberseguridad a través del servicio 24/7 CAI Virtual; solicitud de bloqueo de 7.139 sitios web de contenidos de material de abuso sexual infantil y 1.648 páginas de juegos de azar ilegales; y generación de 454 boletines informativos.

Es de notar que la cooperación se ha realizado de forma activa al lograr la implementación de distintos puestos de mando unificado en materia de seguridad digital liderados desde el Centro de Capacidades para la Ciberseguridad de Colombia a fin de concentrar distintas capacidades en materia de ciberseguridad y ciberdefensa en el territorio nacional.

Desde la referida unidad policial, se ha generado el despliegue de la Estrategia Integral de Ciberseguridad, con el fin de lograr la coordinación activa entre el nivel central de la policía judicial y las 51 unidades desconcentradas de investigación criminal, a fin de estandarizar técnicas de investigación, así como herramientas y mecanismos de cooperación activa.

Según lo informado por la Fiscalía General de la Nación, los delitos informáticos vienen con una tendencia creciente desde 2009, que se acentúo con fuerza en 2019. Es así como, mientras que en 2018 se presentaron 22.238 delitos informáticos, en 2019 se presentaron 24.197, un 9 % más. La tendencia descrita se consolidó durante el año 2020. Entre el 1 de enero y el 31 de diciembre ocurrieron 35.346 delitos informáticos, lo cual representa un aumento del 70 %. Por lo anterior se puede establecer que durante la pandemia sí han aumentado los casos de delitos informáticos en el país.

Por lo anterior, la Fiscalía General de la Nación tiene un canal permanente de comunicación con el Centro Cibernético Policial a través del cual se intercambia información, considerando que éste es el punto de contacto 24/7 según el artículo 35 del Convenio sobre la Ciberdelincuencia.

A fin de mejorar la articulación de las dos entidades, el Centro de Capacidades para la Ciberseguridad de Colombia de la Policía capacitó a los grupos encargados de ciberdelitos de la Fiscalía General de la Nación sobre las capacidades del Centro Cibernético Policial.

Por otro lado, como ya se señaló, a través de las políticas públicas (documento núm. 3995/2020 del Consejo Nacional de Política Económica y Social) se busca fortalecer la política en materia de ciberseguridad y ciberdefensa y la cooperación internacional. Igualmente, se espera mejorar el intercambio de información, la cooperación y la coordinación sólida, efectiva y oportuna entre las partes interesadas en seguridad cibernética a nivel nacional a través de mecanismos de respuesta a crisis como los puestos de mando unificado.

En lo referente a la cooperación, con arreglo al derecho nacional e internacional, respecto de las solicitudes de asistencia de otros Estados para investigar delitos relacionados con las TIC o su uso con fines terroristas o para mitigar las actividades malintencionadas en la esfera de las TIC que se originen en su territorio, conforme lo señala el direccionamiento estratégico 2020–2024 de la Fiscalía General de la Nación, que corresponde al camino trazado por el Fiscal General de la Nación, en el que define integralmente el horizonte de la entidad para los próximos años, la Fiscalía priorizará la investigación de los delitos informáticos. Para ello, se desarrollará una estrategia que permita el fortalecimiento y la articulación de las capacidades investigativas de los investigadores y fiscales que tienen estos casos.

Es así que, a través de una estadística mensual, desde la promulgación de la Ley núm. 1273 de 2009 hasta la fecha, la información relativa a ciberdelitos puede ubicarse en la sección titulada “Datos abiertos de la Fiscalía General de la Nación: consulta y archivos descargables” a partir de parámetros como delitos según lo establecido en el Código Penal Colombiano, el año de entrada de la noticia criminal a la entidad o año en que ocurrieron los hechos, el departamento de ocurrencia de los hechos, el estado y la etapa procesal y el sexo y grupo de edad de víctimas o de indiciados. También el modelo cuenta con identificadores que permiten establecer las noticias criminales que cuentan con formulación de imputación, sentencia condenatoria, órdenes de capturas y archivos por atipicidad o inexistencia.

Los grupos de delitos informáticos de la Fiscalía General de la Nación a nivel nacional en las ciudades principales del país tienen la responsabilidad del procesamiento, análisis y preservación de la evidencia digital, así como de llevar a cabo las diferentes investigaciones de delitos informáticos los cuales, por el lugar de los hechos, son competencia en su jurisdicción, investigaciones de casos como hurto por medios informáticos y pornografía infantil, entre otros. Durante dichas investigaciones, los grupos deben adelantar diligencias de entrevistas, inspecciones, arraigos, labores de verificación, allanamientos, incautaciones, capturas y

acompañamiento de los capturados a las diferentes audiencias. También deben apoyar a todos los despachos de su jurisdicción en la extracción y preservación de evidencia digital de dispositivos o de sitios de Internet de los casos de todos los delitos que así lo requiera, incluidos casos como homicidios, actos sexuales con menores de 14 años, pornografía con menores de 18 años e incluso en ocasiones casos como injuria y calumnia.

En la Dirección de Asuntos Internacionales de la Fiscalía General de la Nación se centralizan todas las asistencias judiciales, en las cuales, en su mayoría, se invoca el Convenio sobre la Ciberdelincuencia, previamente ya aplicados los criterios y filtros que sugiere la *La Guía Práctica para Solicitar la Prueba Electrónica a través de las Fronteras*, elaborada conjuntamente por la Oficina de las Naciones Unidas contra la Droga y el Delito, la Dirección Ejecutiva del Comité contra el Terrorismo y la Asociación Internacional de Fiscales, que fue traducida al español con el apoyo de la OEA.

Por otra parte, desde el Centro de Capacidades para la Ciberseguridad de Colombia, en su calidad de punto de contacto 24/7 del Convenio sobre la Ciberdelincuencia, se ha logrado consolidar a la Policía Nacional como uno de los principales entes de cooperación internacional al tener puntos de contacto en materia de ciberseguridad con importantes agencias como la Agencia de la Unión Europea para la Cooperación Policial e INTERPOL, y fortalecer las distintas instituciones comprometidas en la puesta en práctica de este instrumento de cooperación.

Es de anotar que a través del punto de contacto 24/7 se pretende realizar un trámite más rápido para la atención de solicitudes de asistencia legal mutua, articulando 65 países miembros y 13 países observadores que integran el acuerdo de cooperación.

A continuación, se hará referencia a la recomendación que señala que dada la velocidad a que evolucionan las TIC y el alcance de la amenaza, es necesario afianzar el entendimiento común e intensificar la cooperación. En este sentido, se recomienda que se celebre con regularidad un diálogo institucional con una amplia participación bajo los auspicios de las Naciones Unidas y diálogos en foros bilaterales, regionales y multilaterales y otras organizaciones internacionales.

Al respecto, Colombia continúa participando activamente en los diálogos multilaterales en el marco de las Naciones Unidas y otros foros internacionales, especialmente en lo referido al comportamiento responsable de los Estados en el ciberespacio y los avances de la información y las comunicaciones en el contexto de la seguridad internacional.

Ahora, en el contexto actual de interconexión global sin precedentes, los Estados manejan una relación de interdependencia compleja, compartiendo una serie de problemas conjuntos que por sí solos no podrían solucionar. En ese sentido, los Estados tienen que optar por la cooperación internacional en materia de ciberseguridad, entendiendo que la difusión y el uso de las tecnologías y los medios de información afectan los intereses de toda la comunidad internacional. Por esta razón, los Estados deben promover el uso de las tecnologías de la información y las comunicaciones con fines pacíficos y prevenir conflictos derivados del uso de esas tecnologías que redunda en el interés de todos los Estados. Para ello, se debe:

- Prestar asistencia para crear capacidad en materia de tecnología de la información y las comunicaciones, lo cual es esencial para la seguridad internacional al aumentar la capacidad de los Estados para la cooperación y la acción colectiva, promoviendo la utilización de esas tecnologías con fines pacíficos a partir de la cooperación internacional manejada por el equipo de respuesta a incidentes de ciberseguridad.

- Establecer mecanismos para la participación de los sectores privado, el mundo académico y las organizaciones de la sociedad civil, aportando en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, en el que participan todos los Estados.

Frente a la aplicación de las medidas de cooperación con carácter voluntario en organizaciones bilaterales, multilaterales o regionales, a fin de hacer efectivas la cooperación voluntaria que permita aumentar la confianza para articular las acciones de los Estados contra amenazas nacionales e internacionales derivadas de las tecnologías de la información y las comunicaciones, el Gobierno de Colombia, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, ha:

- Participado en programas regionales como la mesa de ciberseguridad de la Red de Gobierno Electrónico de América Latina y el Caribe, y ha seguido cooperando con la OEA.
- Trabajado desde el año 2017 en el proyecto Trayectoria Profesional en Ciberseguridad, coordinado por el programa de ciberseguridad de la OEA y financiado por la Fundación Citi, el cual busca capacitar a jóvenes de 18 a 25 años de hogares de bajos ingresos y fomentar su preparación profesional en la materia realizado en cinco países: Brasil, Colombia, Costa Rica, Perú y República Dominicana.
- Desarrollado la iniciativa “Hacker Girls”, la cual tiene como propósito apoyar y generar espacios de educación y oportunidad laboral para las mujeres, basados en el fortalecimiento de sus conocimientos en áreas asociadas a la ciberseguridad. Con esta iniciativa, el Ministerio de Tecnologías de la Información y las Comunicaciones avanza en la conformación de un grupo calificado de mujeres expertas en seguridad digital de primer nivel en Colombia que a futuro conformarán el “Colombian Hacker Girls Team”, posicionando al país como líder regional en iniciativas de este tipo, impactando a más de 350 mujeres expertas en seguridad.
- Desarrollado espacios de diálogo a través del Consejo de Innovación en Ciberseguridad, donde se realizaron dos eventos llevados a cabo por expertos regionales y especialistas en pensamiento de diseño (*design thinking*), contando con la participación de directivos de alto nivel de diferentes sectores públicos y privados, gremios y academia, con el fin de impulsar la innovación, concientizar a los participantes y difundir mejores prácticas en materia de ciberseguridad en la región. Estos consejos de innovación están enmarcados dentro de un acuerdo del Programa de Ciberseguridad de la OEA con Cisco y se realizan con el apoyo de la OEA.

En lo referente al compromiso con una acción colectiva que haga de Internet un lugar más seguro, fomentado la asistencia técnica de empresas de tecnología para proteger a los civiles, ya que es en la propiedad privada de los civiles donde principalmente recaen los ataques, el Gobierno de Colombia, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, ha llevado a cabo el programa “EnTIC Confío”, que promueve el desarrollo de las habilidades digitales para enfrentar con seguridad los riesgos asociados al uso de Internet y las TIC. Además de impulsar el uso y la apropiación de Internet como la oportunidad para generar una huella digital positiva en el entorno digital. Este programa va dirigido a mujeres y hombres entre los 6 y los 28 años, y ofrece estrategias diferenciadas en sesiones de trabajo virtuales y presenciales que permiten a sus beneficiarios el desarrollo de habilidades para la identificación de riesgos, la promoción de la convivencia y el activismo digital y la utilización de herramientas tecnológicas para la movilización de causas solidarias y positivas en Internet.

Igualmente, el Gobierno de Colombia, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, está brindando capacitación especializada en seguridad de la información a entidades públicas que soliciten el apoyo del equipo de respuesta a incidentes de ciberseguridad y está ampliando las líneas de investigación en ciberseguridad, fortaleciendo las capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica, específicamente:

– Implementado una guía para la asesoría y acompañamiento para la implementación del habilitador transversal de Seguridad y Privacidad de la Información de las entidades, a partir de la política de Gobierno Digital, cuyas herramientas se basan en: i) el modelo de Seguridad y Privacidad de la Información; y ii) el Modelo de Riesgos de Seguridad Digital – Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública.

– Desarrollado una estrategia de apropiación de la política de seguridad digital definida a través de talleres, charlas de sensibilización, generación de herramientas interactivas y cursos de formación.

– El equipo de respuesta a incidentes de ciberseguridad del Gobierno ofrece servicios proactivos, reactivos y de gestión de la seguridad básicos a todas las entidades del Estado, generando alertas y advertencias sobre amenazas y vulnerabilidades, realizando el tratamiento, análisis, respuesta y coordinación de incidentes, igualmente en el afianzamiento del conocimiento sobre seguridad, generando una cultura de seguridad digital en todos los funcionarios y encargados de seguridad digital.

– Desde el equipo de respuesta a incidentes de ciberseguridad del Gobierno se ha brindado acompañamiento y apoyo a las entidades del Estado, a través de su portafolio de servicios, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica, la gestión de los incidentes cibernéticos y generación de conciencia en seguridad digital. El equipo de respuesta a incidentes de ciberseguridad del Gobierno está integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan acciones tendientes a prevenir y gestionar los incidentes cibernéticos.

Cooperación y asistencia internacionales para promover la seguridad y la creación de capacidad en la esfera de las tecnologías de la información y las comunicaciones

En cuanto a la facilitación de la cooperación transfronteriza para hacer frente a las vulnerabilidades de las infraestructuras fundamentales que trascienden las fronteras nacionales, la Fiscalía General de la Nación ha señalado que en este momento es importante el desarrollo de capacidades en la región para combatir el cibercrimen. Por esto, Colombia ha buscado generar alianzas estratégicas y participación en diferentes escenarios tales como el ingreso oficial como Estado Parte del Convenio sobre la Ciberdelincuencia, la participación en diferentes grupos de trabajo de las Naciones Unidas y la firma de memorandos de entendimiento contra la cibercriminalidad con diferentes Estados.

Por otra parte, en el marco de la cooperación y articulación, Colombia hace parte de la sinergia del equipo de respuesta a incidentes de ciberseguridad en las Américas, espacio para intercambiar información sobre amenazas y la cooperación entre los grupos de respuesta a incidentes de la región.

De igual manera, Colombia participa de los proyectos internacionales de intercambio de información, como boletines y alertas tempranas a entidades gubernamentales y de supervisión de otros países de la región (Consejo

Centroamericano de Superintendentes de Bancos, de Seguros y de otras Instituciones Financieras y Alianza del Pacífico), relacionados con el sector financiero.

La Fiscalía General ha propiciado la suscripción de varios memorandos de entendimiento con otros Estados y a fin combatir la cibercriminalidad y otros delitos conexos.

En relación con la continuación de la labor de creación de capacidades, por ejemplo en técnicas forenses o en medidas de cooperación para hacer frente al uso de las TIC con fines terroristas o delictivos, los esfuerzos en actualización de tecnología y de capacidades ha sido menos rápido debido al alto costo de los licenciamientos, compra de equipos y capacitaciones.

Frente a la recomendación de examinar la posibilidad de elaborar iniciativas de cooperación bilateral y multilateral sobre la base de las relaciones de colaboración ya establecidas en aras de crear capacidad en materia de seguridad en la esfera de las TIC, para ayudar a mejorar el entorno para que los Estados presten una asistencia mutua eficaz a la hora de responder a los incidentes relacionados con las TIC, y las organizaciones internacionales competentes, incluidas las Naciones Unidas y sus organismos, así como el sector privado, el mundo académico y organizaciones de la sociedad civil, el Gobierno de Colombia, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, ha presidido el Comité Ejecutivo de la Red de Gobierno Electrónico de América Latina y el Caribe donde se articulan las autoridades de gobierno digital de 34 países de la región, adelantando temas en materia de ciberseguridad.

Con el propósito de conocer el estado de la ciberseguridad y proponer acciones para su aprobación que mejoren el nivel de ciberseguridad de los países miembros de la Red y de la región, se proponen las siguientes actividades:

– Nivel de madurez en ciberseguridad (estudio del Banco Interamericano de Desarrollo y la OEA).

– Nivel de madurez de los equipos de respuesta a emergencias informáticas y equipos de respuesta a incidentes de ciberseguridad (SIM3).

– Repositorio de guías, procedimientos y buenas prácticas de ciberseguridad.

– Evento de ciberseguridad para tomadores de decisión.

– Estrategias de ciberseguridad regionales.

– Desarrollo de buenas prácticas voluntarias regionales en manejo de datos sensibles (fortalecer firma digital transfronteriza y la interoperabilidad).

– Estudio del estado de los equipos de respuesta a incidentes de ciberseguridad de los miembros de la Red.

– Desarrollo de equipos de respuesta a incidentes de ciberseguridad por sectores y colaboración de la región.

– Desarrollo de capacidades en ciberseguridad.

– Desarrollo de capacidades de los equipos de respuesta a incidentes de ciberseguridad.

– Plataforma de intercambio de información sobre malware (equipo de respuesta a incidentes de ciberseguridad en las Américas).

– Análisis de marcos de protección de datos regionales.

Adicionalmente, el Gobierno de Colombia ha implementado, en convenio con la OEA y el Ministerio de Tecnologías de la Información y las Comunicaciones, una

serie de propuestas del modelo de gobernanza de seguridad digital y una guía metodológica para la identificación y gestión de riesgos de seguridad digital en la adopción de tecnologías emergentes para Colombia. En el marco de esta propuesta se avanzó en:

– La compilación de fuentes y referentes para ambos productos a proponer.

– El análisis de mejores prácticas para ambos productos de aprendizaje por comparación (benchlearning) sobre modelos de gobernanza aplicables a la seguridad digital.

– El análisis de contexto local (institucionalidad, partes interesadas, etc.).

– La formulación de propuesta de principios y objetivos del modelo de gobernanza.

– La validación de la propuesta de objetivos y obtención de sugerencias de múltiples partes interesadas respecto al modelo de gobernanza.

– La identificación de expectativas de las diferentes partes interesadas respecto al modelo de gobernanza.

Es de anotar que, para la validación de las propuestas de principios y objetivos, así como de los intereses de las diferentes partes interesadas respecto al modelo de gobernanza, en Colombia se llevó a cabo una primera mesa de trabajo en el marco de la sesión formal del Comité de Seguridad Digital realizada el 30 de octubre de 2020, que contó con más de 80 participantes, representantes de las múltiples partes interesadas en el ecosistema de ciberseguridad nacional.

Frente a la posibilidad de construir una plataforma que permita la cooperación operativa no solo entre Estados sino también con el sector privado nacional, permitiendo que se afronte y responda a los incidentes y crisis cibernéticas a gran escala, el Gobierno de Colombia, en cabeza del Ministerio de Defensa Nacional, trabaja en desarrollar lo dispuesto en el plan de acción del documento 3995/2020 del Consejo Nacional de Política Económica y Social:

a) Establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital.

b) Adoptar modelos con énfasis en nuevas tecnologías, haciendo necesario desarrollar la implementación tecnológica del Sistema Nacional de Gestión de Incidentes Cibernéticos, con el fin de articular los esfuerzos institucionales para la gestión oportuna de los incidentes cibernéticos, y lograr tener la fuente oficial de las estadísticas de los incidentes cibernéticos reportados en el país.

c) Estandarizar un mecanismo de reporte periódico de incidentes y vulnerabilidades cibernéticas que permita identificarlos, evaluarlos y comunicarlos a los interesados y sirva de fuente para la toma de decisiones por parte del Gobierno Nacional.

Aplicación del derecho internacional al uso de las tecnologías de la información y las comunicaciones

Colombia considera que el derecho internacional aplica “en espacio virtual”, al igual que rige para el “espacio físico”, en particular la Carta de las Naciones Unidas, e incluyendo el derecho internacional de los derechos humanos y el derecho internacional humanitario en cuanto este último sea aplicable. Ello por cuanto el

derecho internacional humanitario sólo se aplica en situaciones de conflicto armado (en el espacio físico o virtual).

El derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la paz y la estabilidad y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico. Por lo que el principio de la igualdad soberana se sustenta como base para una mayor seguridad en el uso de las TIC por los Estados, y es preciso observar, entre otros principios del derecho internacional, la soberanía del Estado, la igualdad soberana, la solución de controversias por medios pacíficos y la no intervención en los asuntos internos de otros Estados.

Conceptos

En relación con la profundización de los conceptos relativos a la paz y la seguridad internacionales en el uso de las TIC en el plano jurídico, técnico y político, dadas las particularidades y la novedad de su aplicación, se considera que éstos deberán continuar siendo discutidos en el marco de los escenarios multilaterales, siguiendo las conclusiones del informe final del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, adoptado por consenso en marzo de 2021.

Para poder profundizar en el tema de la aplicación del derecho internacional en el ciberespacio, es fundamental contar con herramientas de construcción de capacidades para que todos los Estados puedan hablar el mismo lenguaje y avanzar en estos entendimientos que permitan ajustar la normatividad internacional a los desafíos del ciberespacio y poder generar consensos alrededor de cómo se aplica el derecho internacional en este espacio virtual.

Se resalta la importancia de que se avance en la implementación de las recomendaciones tanto de los Grupos de Expertos Gubernamentales, como del Grupo de Trabajo de Composición Abierta.

Adicionalmente, se resalta la importancia de que se establezca el mecanismo global de diálogo institucional periódico en el marco de Naciones Unidas para avanzar en ese sentido, y de que se continúe y fortalezca la labor que se lleva a cabo a nivel regional.

En ese sentido, Colombia apoya y copatrocina la iniciativa de un programa de acción sobre el uso responsable de las TIC en el contexto de la seguridad internacional, como un instrumento internacional permanente, inclusivo, consensuado y orientado a la acción para promover un comportamiento responsable en el uso de las TIC en el contexto de la seguridad internacional.

Dinamarca

[Original: inglés]
[28 de mayo de 2021]

En Dinamarca, como en muchas partes del mundo, las soluciones digitales forman parte de la vida cotidiana y ayudan a impulsar el crecimiento económico. Como uno de los países más digitalizados del mundo, es vital que Dinamarca impulse un ciberespacio mundial, abierto, libre, estable, pacífico y seguro en el que se apliquen plenamente los derechos humanos y las libertades fundamentales, así como el estado de derecho.

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

Dinamarca ha adoptado varias medidas para fortalecer la seguridad de la información y promover la cooperación internacional en el ciberespacio.

El Acuerdo de Defensa para 2018-2023 asigna 1.400 millones de coronas danesas al fortalecimiento de la ciberseguridad y la ciberdefensa, reforzando así la capacidad de resiliencia de Dinamarca. La Estrategia Danesa de Seguridad Cibernética y de la Información de 2018-2021 adopta nuevas medidas para aumentar la seguridad cibernética y de la información y garantizar un esfuerzo sistemático y coordinado. Mediante 25 iniciativas y 6 estrategias específicas que abordan lo que hasta ahora se ha definido como sectores críticos (energía, finanzas, transporte, atención de la salud, telecomunicaciones y sector marítimo), Dinamarca ha aumentado la resiliencia tecnológica de su infraestructura digital, ha mejorado los conocimientos y aptitudes de los ciudadanos, las empresas y las autoridades, y ha fortalecido la coordinación y la cooperación en materia de ciberseguridad.

En el marco de la Estrategia Danesa de Seguridad Cibernética y de la Información de 2018-2021, se han establecido unidades dedicadas a la ciberseguridad y la seguridad de la información en los seis sectores críticos antes mencionados. Además, la estrategia nacional estableció un foro para las unidades sectoriales especializadas y el Centro de Ciberseguridad, centrándose en el intercambio de su experiencia en el trabajo con la ciberseguridad y la seguridad de la información. La Agencia de Digitalización y el Servicio de Seguridad e Inteligencia de Dinamarca también participan en el foro.

A fin de contar con personal suficientemente capacitado para detectar y manejar los ciberataques contra Dinamarca, en particular en lo que respecta a la infraestructura crítica, el Centro de Ciberseguridad ha desarrollado y puesto en marcha además su propia Ciberacademia intensiva. Además de la Academia, el Centro de Ciberseguridad también apoya la educación y la investigación en el ámbito de la ciberseguridad.

Además de esas iniciativas, la Agencia de Digitalización ha desarrollado y ejecutado varios cursos, material educativo y eventos sobre ciberseguridad y seguridad de la información dirigidos al nivel de los jefes ejecutivos y a los especialistas en cibernética, así como a los empleados públicos.

Como parte de la Estrategia Danesa de Seguridad Cibernética y de la Información de 2018-2021, la Agencia de Digitalización ha desarrollado el sitio web sikkerdigital.dk, que ofrece a los ciudadanos orientación, artículos y herramientas de aprendizaje sobre ciberseguridad y seguridad de la información y conocimientos sobre diferentes amenazas. Además del sitio web, la Agencia de Digitalización lleva a cabo campañas nacionales sobre el comportamiento digital seguro en cooperación con los municipios y las regiones.

Dinamarca también cuenta con un Consejo de Ciberseguridad público-privado, creado para asesorar al Gobierno sobre la manera de reforzar la ciberseguridad y mejorar el intercambio de conocimientos entre autoridades, empresas e investigadores. Con la Estrategia Danesa de Seguridad Cibernética y de la Información 2018-2021, Dinamarca también ha fortalecido su cibercompromiso internacional mediante el envío de ciberagentes a Bruselas; el nombramiento de un cibercoordinador internacional en el Ministerio de Relaciones Exteriores; el nombramiento de un asesor de ciberseguridad en la Oficina del Embajador de Tecnología en Silicon Valley; y la adhesión al Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) en Tallin. Esto ha permitido a Dinamarca intensificar su participación en ciberforos

multilaterales, como los de las Naciones Unidas, la Unión Europea, la OTAN y la Organización para la Seguridad y la Cooperación en Europa (OSCE).

El Gobierno de Dinamarca está trabajando actualmente en una nueva estrategia de seguridad cibernética y de la información para 2022-2024. La estrategia se basará en los esfuerzos actuales y los ampliará reforzando la ciberseguridad y la seguridad de la información mediante iniciativas dirigidas a los sectores público y privado y a los ciudadanos daneses.

Al mismo tiempo, Dinamarca mantiene su 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. El aumento de los ataques y las operaciones durante la pandemia de enfermedad por coronavirus (COVID-19) ha dado lugar a esfuerzos diplomáticos sostenidos 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. Además, Dinamarca es miembro activo del Grupo de Cooperación en materia de Seguridad de la Información en las Redes y de la red de Equipos de Respuesta a Incidentes de Seguridad Informática y es miembro de la junta de la Agencia de la Unión Europea para la Ciberseguridad.

Dinamarca subraya que, como ha dejado claro la comunidad internacional, el ciberespacio está firmemente arraigado en el derecho internacional vigente, como han atestiguado los informes de los Grupos de Expertos Gubernamentales aprobados por consenso de 2013 y 2015. 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 y es fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de la tecnología de la información y las comunicaciones (TIC). Dinamarca destaca además la importancia de 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, como complementarias del derecho internacional existente y derivadas de este.

A pesar de nuestros esfuerzos nacionales e internacionales, la capacidad y la voluntad de los agentes estatales y no estatales de realizar ciberactividades malintencionadas siguen aumentando. Eso debería ser una preocupación mundial. Las actividades malintencionadas en el ciberespacio pueden constituir hechos ilícitos con arreglo al derecho internacional además de ser desestabilizadoras y entrañar el riesgo de una escalada. Dinamarca sigue decidida a prevenir, disuadir y responder a las actividades malintencionadas y a tratar de mejorar la cooperación internacional a tal efecto. Dinamarca se suma a la Unión Europea para pedir a la comunidad internacional que refuerce 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.

Contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales

Amenazas existentes y nuevas amenazas

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.

Nunca antes la necesidad de un ciberespacio mundial, libre, abierto, seguro, estable y pacífico ha sido tan evidente como durante la pandemia de COVID-19. Las TIC permiten la comunicación, la colaboración y el intercambio de conocimientos que el mundo necesita para hacer frente a la pandemia.

No obstante, durante la actual crisis de la COVID-19, hemos visto que los agentes malintencionados aprovechan cualquier oportunidad, incluso una pandemia mundial. Esto incluye la interferencia con la infraestructura crítica, como los hospitales que son esenciales para luchar contra la pandemia, y el robo de propiedad intelectual facilitado por medios cibernéticos. Cualquier intento de obstaculizar la capacidad de las infraestructuras críticas 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. Esto es inaceptable y debe ser condenado enérgicamente por todos los Estados. Además, los Estados deben ejercer la debida diligencia y adoptar medidas rápidas y firmes contra la actividad malintencionada de las TIC que tiene origen en su territorio.

Además, como se reconoció en informes anteriores del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, dado el carácter único de las TIC, el enfoque adoptado por las Naciones Unidas y 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.

La comunidad internacional ha dejado claro que el ciberespacio está firmemente arraigado en el derecho internacional vigente, como atestiguan también los informes de los Grupos de Expertos Gubernamentales aprobados por consenso de 2013 y 2015. 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. Dinamarca se congratula de que este año la Asamblea General llegara por consenso a esta conclusión cuando hizo suyo el informe final del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Ahora todos los Estados Miembros deben hacer honor a ese 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 hay margen para fortalecer el entendimiento y la interpretación comunes de estos principios fundamentales, y Dinamarca apoya la labor del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de

Composición Abierta, y otras iniciativas internacionales y regionales para lograr este resultado, como un nuevo programa de acción a fin de promover un comportamiento responsable de los Estados en el ciberespacio.

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 para las Operaciones Militares en el Ciberespacio de 2019, en la que se obliga a los dirigentes militares 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 al ciberespacio. Cabe esperar que la labor y las recomendaciones del actual Grupo de Expertos Gubernamentales y del nuevo Grupo de Trabajo de Composición Abierta contribuyan a aclaraciones adicionales y faciliten así el cumplimiento por parte de los Estados, así como que promuevan una mayor previsibilidad y reduzcan el riesgo de escalada.

Normas, reglas y principios para el comportamiento responsable de los Estados

Dinamarca se suma a la Unión Europea y a sus Estados miembros para alentar a todos los Estados a que aprovechen y promuevan la labor que la Asamblea General ha hecho suya en repetidas ocasiones, en particular en su resolución 70/237, y a que sigan aplicando esas normas y medidas de fomento de la confianza convenidas, que desempeñan un papel esencial en la prevención de conflictos.

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 de los Grupos de Expertos Gubernamentales en 2010, 2013 y 2015 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.

República de Moldova

[Original: inglés]
[24 de mayo de 2021]

Las tecnologías de la información, los recursos informáticos y los sistemas de comunicación electrónica se han convertido en una parte indispensable de todos los ámbitos de actividad de la persona, la sociedad y el Estado. Las tecnologías de la información contribuyen a las transformaciones esenciales del orden social y sirven como generadoras de una sociedad informacional consolidada a nivel nacional, regional e internacional. Por lo tanto, las tecnologías de la información han superado el marco jurídico de las fronteras estatales o de las comunidades de Estados.

Además de las ventajas indiscutibles de las tecnologías modernas, el espacio de la información está expuesto a varias amenazas de seguridad. Así, facilita la competitividad desleal, el espionaje, la desinformación masiva, la propaganda, el terrorismo y la delincuencia organizada, la difusión de formas de odio y la incitación a la violencia, especialmente por criterios de género, raza, nacionalidad, origen étnico, lengua, religión, afiliación política y otros, actuaciones que siguen siendo subestimadas y que raramente se remedian o contrarrestan.

La política nacional para garantizar la seguridad de la información de un Estado de derecho tiene como prioridades básicas un aumento del nivel de seguridad de la información y la creación de condiciones favorables para determinadas actividades de los agentes públicos y privados, incluidos los simples usuarios de los sistemas de información. La realización de estas acciones implica la existencia de un marco normativo actualizado y completo, que abarque las principales cuestiones en el ámbito de la seguridad de la información. A este respecto, en la República de Moldova se han aprobado la Estrategia de Seguridad de la Información y el Plan de Actividades para su aplicación. Por tanto, el objetivo de la Estrategia es garantizar la protección de los derechos y libertades fundamentales, la democracia y el estado de derecho en el espacio informativo.

La clasificación de los riesgos, amenazas y vulnerabilidades, así como la sistematización de las actividades que garantizan la seguridad de la información, contribuyen a aumentar el nivel de confianza en el ciberespacio, hecho que se refleja en la Estrategia de Seguridad de la Información de la República de Moldova.

El objetivo de la Estrategia es correlacionar desde el punto de vista jurídico e integrar sistémicamente los ámbitos prioritarios con las responsabilidades y competencias para garantizar la seguridad de la información a nivel nacional sobre la base de la ciberresiliencia, el pluralismo multimedia y la convergencia institucional en el ámbito de la seguridad con el objetivo de proteger la soberanía, la independencia y la integridad territorial de la República de Moldova.

De esa forma, la Estrategia proporciona mecanismos concretos y claros para identificar, contrarrestar y responder a las amenazas a la seguridad de la información, así como los plazos para alcanzar los objetivos de su aplicación.

Los mecanismos y objetivos incluidos en la Estrategia están orientados a la creación y actualización del marco normativo y a la puesta en marcha de los componentes técnicos programáticos y de ejecución que harán frente a los retos internos y externos del país, a la formación del personal y a la intensificación de la cooperación con los organismos nacionales e internacionales competentes.

En este sentido, la Estrategia prevé la creación de un sistema integrado de comunicación y evaluación de las amenazas a la seguridad de la información y la elaboración de medidas operativas de respuesta. Esto entraña la creación o designación de una entidad como centro nacional de respuesta a incidentes de

ciberseguridad que sería el punto único para que las autoridades públicas competentes y las personas físicas y jurídicas denunciasen incidentes de ciberseguridad. La creación de un equipo nacional de respuesta a emergencias informáticas reforzaría la red de equipos en el territorio de la República de Moldova y garantizaría una respuesta rápida a los incidentes.

Además, teniendo en cuenta la necesidad de realizar una vigilancia constante y de garantizar un alto nivel de ciberseguridad, la Estrategia prevé la realización de una auditoría de las infraestructuras de tecnología de la información de interés nacional y la aplicación de normas internacionales de seguridad de la información.

Además, la Estrategia establece mecanismos de protección para las redes de comunicación especiales de la República de Moldova y para la información de acceso restringido. Los sistemas de comunicación, los sistemas de información y las redes de transmisión de datos están concebidos para el almacenamiento, el tratamiento y la posterior transmisión de datos importantes para el Estado, por lo que requieren un enfoque específico en cuanto a su protección y desarrollo.

El creciente número de medios de protección criptográfica y la complejidad de los algoritmos criptográficos hacen necesario garantizar el control de la importación, la certificación y la utilización de los medios de protección de la información. Por ello, la Estrategia exige la certificación de los medios técnicos y criptográficos de protección de la información, el desarrollo de sistemas de control de la importación de medios de protección de la información, la adecuación al marco jurídico europeo del marco jurídico nacional en materia de protección de la información criptográfica y la creación de una base de datos sobre medios técnicos y criptográficos de protección de la información.

Además, el libre acceso a la red global de Internet, la existencia de datos de carácter pornográfico y extremista, junto con la dificultad de establecer la fuente y la veracidad de los datos que se cargan en línea, hacen necesario el desarrollo de mecanismos de protección para los usuarios, especialmente los niños, contra cualquier forma de abuso en el espacio en línea.

A fin de identificar, contrarrestar y responder a las amenazas a la seguridad de la información en el ámbito de los medios de comunicación informativos, era necesario realizar una evaluación del espacio de Internet para identificar las entidades y/o personas implicados en la producción y difusión en línea de contenidos de los medios de comunicación que afectaran a la seguridad de la información de la República de Moldova.

Asimismo, para desarrollar mecanismos de comunicación estratégica, promover los intereses nacionales de la República de Moldova y garantizar la seguridad del espacio de la información en los medios de comunicación, la Estrategia prevé la realización de un estudio exhaustivo destinado a detectar y evaluar los elementos vulnerables del componente mediático dentro del sistema de seguridad de la información, así como la creación de un recurso informativo para la comunicación estratégica que contenga información sobre incidentes de seguridad y sobre los intentos de desinformación o manipulación detectados.

Además, cabe mencionar que la Estrategia contiene objetivos necesarios para la cooperación internacional en el ámbito de la seguridad de la información y la lucha contra los delitos cibernéticos.

La Estrategia de Seguridad de la Información se aprobó para el período comprendido entre 2019 y 2024 y establece una serie de objetivos y medidas que deben alcanzarse gradualmente, en particular con la ayuda de socios internacionales.

A pesar de que a nivel nacional, la República de Moldova está tratando de implementar varias medidas para consolidar sus capacidades de seguridad de la información, consideramos que a nivel internacional la situación en el ciberespacio es cada vez más compleja, con actores estatales malintencionados que realizan sofisticados ciberataques para interferir en los procesos electorales de otros países, dañando infraestructuras vitales y llevando a cabo ataques de ciberespionaje del tipo "cadena de suministro", todo lo cual es contrario a las resoluciones de las Naciones Unidas.

Al mismo tiempo, los ciberagentes no estatales explotan plenamente las vulnerabilidades de los sistemas de información con fines delictivos para obtener beneficios económicos, utilizando instrumentos de "programas malignos como servicio".

Los problemas mencionados hacen que la población sea reticente a las nuevas tecnologías y representan un impedimento para el buen desarrollo de las tecnologías de la información.

Singapur

[Original: inglés]
[24 de mayo de 2021]

Singapur está firmemente comprometido con el establecimiento 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. Es importante que los debates sobre esas leyes, reglas y normas sigan teniendo lugar en las Naciones Unidas, que es el único foro universal, inclusivo y multilateral en que 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 durante el período de 2019 a 2021 y en el recientemente concluido Grupo de Trabajo de Composición Abierta establecido en virtud de la resolución 73/27 de la Asamblea General. Seguimos comprometidos a contribuir de forma constructiva a la labor de las Naciones Unidas para desarrollar y aplicar normas y reglas sobre ciberseguridad y seguiremos participando activamente en futuros procesos de las Naciones Unidas. En nuestra opinión, es importante que los futuros debates sobre ciberseguridad en las Naciones Unidas tengan en cuenta una amplia gama de puntos de vista, especialmente de los Estados pequeños y los países en desarrollo que son especialmente vulnerables a los efectos de los ciberconflictos. Con este fin, cualquier proceso futuro de las Naciones Unidas sobre ciberseguridad debe ser abierto, inclusivo y colaborativo con el fin de fortalecer aún más la cooperación internacional y avanzar en la promoción del 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.

Singapur considera que los Estados deben promover la sensibilización sobre las normas voluntarias y no vinculantes existentes sobre el comportamiento responsable de los Estados y apoyar su aplicación. Singapur es partidario de que se sigan

elaborando ese tipo de normas cuando sea necesario. Por ejemplo, las infraestructuras transfronterizas de información crítica, 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 las TIC a dichas infraestructuras podrían tener efectos desestabilizadores a nivel regional y mundial[2].

Las organizaciones regionales pueden desempeñar un importante papel. La Asociación de Naciones de Asia Sudoriental (ASEAN) reafirmó la necesidad de establecer un orden internacional basado en normas en el ciberespacio en la primera declaración de los dirigentes de la ASEAN sobre la cooperación en materia de ciberseguridad, publicada en abril de 2018. En septiembre de 2018, los participantes de la Tercera Conferencia Ministerial de la ASEAN sobre Ciberseguridad acordaron suscribir en principio las 11 normas del informe de 2015 del Grupo de Expertos Gubernamentales, y centrarse en el fomento de la capacidad regional para aplicar esas normas. En octubre de 2019, los participantes en la Cuarta Conferencia Ministerial de la ASEAN sobre Ciberseguridad decidieron establecer un comité de trabajo para examinar la elaboración de un plan de acción regional a largo plazo para garantizar la aplicación efectiva y práctica de las normas, en particular en las esferas de la cooperación entre los equipos de respuesta a emergencias informáticas, la protección de la infraestructura de información crítica y la asistencia mutua en materia de ciberseguridad. Los participantes en la Quinta Conferencia Ministerial de la ASEAN sobre Ciberseguridad, celebrada en 2020, reiteraron el compromiso de la ASEAN de desarrollar un plan de acción para trazar la hoja de ruta de aplicación de las normas a un ritmo adecuado para todos los Estados miembros de la ASEAN. Los participantes también coincidieron en la urgente necesidad de proteger las infraestructuras críticas de información nacionales y transfronterizas.

El fomento de la capacidad es esencial para asegurar que los Estados individuales desarrollen la capacidad de aplicar con éxito las normas de comportamiento responsable de los Estados y las obligaciones que les incumben en virtud del derecho internacional. Como parte de este esfuerzo, Singapur estableció en 2016 el Programa de Capacidad Cibernética de la ASEAN para apoyar la creación de capacidad en los países de la ASEAN en materia de políticas relacionadas con la cibernética, así como de cuestiones operativas y técnicas. Hasta la fecha, el Programa de Capacidad Cibernética de la ASEAN ha formado a más de 600 funcionarios de los Estados miembros de la ASEAN. Como una extensión del Programa, el Centro de Excelencia sobre Ciberseguridad de la ASEAN-Singapur se lanzó en 2019 con un compromiso de 30 millones de dólares de los Estados Unidos para ofrecer programas políticos y técnicos para altos funcionarios de la ASEAN. El Centro de Excelencia está en funcionamiento desde abril de 2020. A pesar de las restricciones a los viajes derivadas de la pandemia de COVID-19, el Centro de Excelencia continuó con sus programas de formación en línea y organizó siete programas virtuales de capacitación en 2020.

Singapur también coorganizó un taller en el marco del programa cibernético de las Naciones Unidas en Singapur para crear conciencia sobre las normas cibernéticas entre los Estados miembros de la ASEAN. Además, Singapur se asoció con la Oficina de Asuntos de Desarme para elaborar un curso insignia de capacitación en línea abierto a todos los Estados Miembros de las Naciones Unidas. El curso tiene por objeto promover una mayor comprensión del uso de las tecnologías de la información y las comunicaciones y sus repercusiones en la seguridad internacional. Seguimos

[2] Las infraestructuras transfronterizas de información crítica son tecnologías de información esenciales que pertenecen a empresas privadas y operan a través de las fronteras nacionales, pero no bajo la jurisdicción de un solo Estado.

comprometidos a compartir nuestra experiencia y conocimientos con los Estados Miembros de las Naciones Unidas, especialmente con los pequeños países en desarrollo.

En el plano nacional, Singapur ha seguido fortaleciendo la ciberseguridad de sus sistemas y redes en tres frentes, a saber, la construcción de una infraestructura resiliente, la creación de un ciberespacio más seguro y el desarrollo de un ecosistema de ciberseguridad dinámico:

a) *Construcción de una infraestructura resiliente.* La Agencia de Ciberseguridad de Singapur puso en marcha en 2019 el Plan Maestro de Ciberseguridad de la Tecnología Operacional como parte de nuestros esfuerzos por mejorar la seguridad y la resiliencia de los sectores de infraestructura de información crítica 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. En 2021, la Agencia de Ciberseguridad desarrollará y pondrá en marcha un programa para las cadenas de suministro de infraestructuras de información críticas, en el que participarán las partes interesadas, incluidos los organismos gubernamentales, los 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;

b) *Creación de un ciberespacio más seguro.* Como parte de nuestros esfuerzos a fin de reforzar la actitud nacional ante la ciberseguridad en Singapur, la Agencia de Seguridad Cibernética lanzó en 2020 el Plan Maestro por un Ciberespacio más Seguro para: i) asegurar nuestra infraestructura digital fundamental; ii) salvaguardar nuestras actividades en el ciberespacio; y iii) empoderar a nuestra población familiarizada con las cuestiones cibernéticas. El Plan Maestro esboza 11 iniciativas destinadas a aumentar la adopción de la seguridad mediante el 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. Una de estas iniciativas es el Plan de Etiquetado de Ciberseguridad para los dispositivos inteligentes conectados a la red. Se puso en marcha en 2020 como un plan voluntario para dar tiempo al mercado y a los desarrolladores para entender qué beneficios puede reportarles el Plan. Las etiquetas de ciberseguridad proporcionarán una indicación del nivel de seguridad incorporado en los productos. Los consumidores pueden elegir productos con mejores calificaciones de seguridad utilizando la información de la etiqueta de ciberseguridad. El Plan tiene por objeto incentivar a los fabricantes a que desarrollen y ofrezcan productos con características de ciberseguridad reconocidas y mejoradas;

c) *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. 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 de Ciberseguridad 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.

Suiza

[Original: inglés]
[28 de mayo de 2021]

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

Suiza ha adoptado una serie de medidas a nivel nacional, regional y mundial destinadas a promover un ciberespacio más estable, abierto y libre.

La Estrategia de Política Exterior de Suiza 2020-2023[3] establece las líneas generales y las prioridades, incluido el compromiso continuo de Suiza por un espacio digital abierto y seguro que se base en el derecho internacional y se centre en las personas y sus necesidades. Suiza también se ha comprometido a reforzar la posición de Ginebra como centro líder en el mundo en materia digital. La primera Estrategia de Política Exterior Digital de Suiza 2021-2024[4] toma como base la Estrategia de Política Exterior y establece principios clave destinados a garantizar un espacio digital abierto, libre y seguro.

La segunda Estrategia Nacional para la Protección de Suiza contra los Riesgos Cibernéticos 2018-2022 se basa en los objetivos estratégicos esbozados en la primera Estrategia Nacional para la Protección de Suiza contra los Riesgos Cibernéticos de 2012[5]. Ambas Estrategias reconocen la importancia de las tecnologías de la información y las comunicaciones (TIC) como motores indispensables de las actividades sociales, económicas y políticas, y sientan las bases de un enfoque global, integrado y holístico para hacer frente a las amenazas basadas en las TIC. Suiza pretende mejorar su detección temprana de riesgos cibernéticos y amenazas emergentes, aumentar la resiliencia de sus infraestructuras críticas y, en general, reducir los riesgos cibernéticos. El fundamento de las estrategias es la necesidad de una cultura de la ciberseguridad, la responsabilidad compartida entre los diferentes niveles de gobierno y entre los sectores público y privado, así como la necesidad de un enfoque basado en los riesgos. Las Estrategias abogan por una mayor coordinación a nivel gubernamental y fomentan las alianzas público-privadas y una mayor cooperación en el ámbito internacional. Se estableció que la cooperación, ya sea a nivel nacional o internacional, era una de las piedras angulares del enfoque de Suiza para hacer frente a las ciberamenazas. En 2019 se creó el Centro Nacional de Ciberseguridad, que sirve de punto de contacto para las empresas, el mundo académico, el público en general y los organismos gubernamentales. Está dirigido por el Delegado Federal de Ciberseguridad y contribuye también a aumentar la concienciación sobre la ciberseguridad.

En septiembre de 2020, el Consejo Federal adoptó la nueva Estrategia Digital de Suiza[6]. Esta identifica una serie de campos de acción para la cooperación entre el Gobierno, el mundo académico, el sector privado y la sociedad civil con el fin de dar

[3] Puede consultarse en: www.eda.admin.ch/eda/en/fdfa/foreign-policy/implementing-foreign-policy/aussenpolitischestrategie.html.
[4] Puede consultarse en: www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2020/11/digitalaussenpolitik-strategie.html.
[5] Puede consultarse en: www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html.
[6] Puede consultarse en: www.digitaldialog.swiss/en/.

forma a la transformación digital de nuestra sociedad en beneficio de todos en Suiza y para garantizar que las oportunidades que presenta estén disponibles para todos.

En marzo de 2021, el Departamento Federal de Defensa aprobó su Estrategia de Ciberdefensa 2021-2024[7]. La Estrategia tiene como objetivo la anticipación y la detección temprana de ciberamenazas y actividades malintencionadas, la prevención y la atribución de ciberincidentes cuyo blanco sean los intereses de Suiza y la educación y formación del personal civil y militar, así como la ciberresiliencia de las infraestructuras críticas.

En cuanto a la protección de las infraestructuras críticas, Suiza sigue un enfoque descentralizado. El mandato relativo a la protección de las infraestructuras críticas se asigna a varios departamentos y oficinas federales, como la Oficina Federal de Protección de la Población, la Oficina Federal de Aprovisionamiento Económico Nacional y el Servicio Federal de Inteligencia, por lo que no se limita a un único organismo.

Desde la adopción de las Estrategias Nacionales para la Protección de Suiza contra los Riesgos Cibernéticos, se han desarrollado aún más las capacidades destinadas a establecer la autoría de las actividades cibernéticas malintencionadas. La identificación de los autores sigue un enfoque holístico que incluye el análisis de las características técnicas de un ciberincidente, tiene en cuenta el contexto geopolítico y utiliza todo el conjunto de fuentes de inteligencia para obtener información relevante. Suiza ha definido un proceso estandarizado interinstitucional para atribuir públicamente (atribución política) un ciberincidente que suponga una amenaza para la seguridad nacional de Suiza. Los criterios de atribución jurídica de un ciberincidente según el derecho internacional forman parte de esta evaluación.

En enero de 2019, Suiza creó un “Campus de Ciberdefensa”[8] que lleva a cabo investigaciones para predecir y vigilar las posibles amenazas derivadas de los avances tecnológicos, propone soluciones y forma a ciberexpertos. El Campus reúne a expertos de la Oficina Federal de Armamento, la industria y las instituciones de investigación.

En cuanto a la divulgación y colaboración con el sector privado y el mundo académico, Suiza fomenta diversas iniciativas. Por ejemplo, para contrarrestar las actividades de espionaje y proliferación, el Servicio Federal de Inteligencia ha utilizado, desde 2004, su programa de campañas de prevención y concienciación “Prophylax” para asesorar a empresas, universidades e institutos de investigación sobre posibles medidas preventivas para identificar las actividades ilegales de espionaje y proliferación y responder a ellas.

Contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales

En cuanto a la evaluación de las amenazas, las actividades cibernéticas malintencionadas dirigidas directamente a las infraestructuras críticas pueden causar graves daños y tener un impacto negativo en el funcionamiento de los servicios esenciales, como la asistencia sanitaria. En los últimos años, varios organismos federales y empresas privadas suizos han sido víctimas de ciberactividades malintencionadas patrocinadas por Estados (ciberespionaje). El objetivo final de estas actividades cibernéticas malintencionadas suele ser obtener ventajas económicas, políticas y militares. En el transcurso de 2020, varias infraestructuras críticas de Suiza se vieron afectadas principalmente por ataques con motivación financiera. En el

[7] Puede consultarse en: www.newsd.admin.ch/newsd/message/attachments/66203.pdf.

[8] Véase www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

futuro, Suiza espera un aumento de los ataques con programas secuestradores por parte de grupos delictivos, así como de las ciberoperaciones dirigidas, patrocinadas o consentidas por los Estados. Además, las ciberactividades maliciosas pueden tener efectos no deseados en Suiza y provocar daños colaterales. Como los agentes generadores de amenazas siguen desarrollando técnicas y herramientas para socavar y manipular el *software* legítimo, los ataques a la cadena de suministro son especialmente preocupantes.

Suiza participó y contribuyó activamente en el sexto Grupo de Expertos Gubernamentales (2019 a 2021) y en el Grupo de Trabajo de Composición Abierta (2019 a 2021), en lo relativo a la ciberestabilidad internacional y el fortalecimiento de la aplicación del marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio. Suiza está convencida de que la aplicación del derecho internacional, incluidos el derecho de los derechos humanos y el derecho internacional humanitario, las normas voluntarias no vinculantes, las medidas de fomento de la confianza y el fomento de la capacidad son fundamentales para garantizar y mantener la ciberseguridad internacional. El Representante Permanente de Suiza ante las Naciones Unidas en Nueva York presidió el Grupo de Trabajo de Composición Abierta. Bajo su Presidencia, el Grupo acordó un informe final consensuado en marzo de 2021 (A/75/816).

Suiza está comprometida con la Unión Internacional de Telecomunicaciones, en particular en sus consultas sobre las directrices para la utilización de la Agenda sobre Ciberseguridad Global, con el objetivo de crear coherencia con otros procesos a nivel de las Naciones Unidas.

Suiza está comprometida con la promoción del papel de la Organización para la Seguridad y la Cooperación en Europa (OSCE) en el fomento de la ciberestabilidad y participa activamente en su grupo de trabajo oficioso sobre ciberseguridad. Desde el establecimiento del mandato de la OSCE para elaborar y aplicar medidas de fomento de la confianza, Suiza ha aumentado la transparencia de su propia postura frente a las cuestiones cibernéticas compartiendo información sobre las estructuras, organizaciones y políticas nacionales en las reuniones periódicas del grupo de trabajo oficioso, a través de las plataformas mantenidas por la OSCE y la Red de Comunicaciones de la OSCE. Junto con Alemania, Suiza también ha continuado su compromiso para hacer operativo el mecanismo de información y consulta consagrado en la medida de fomento de la confianza núm. 3.

Suiza es uno de los Estados partes en el Convenio sobre la Ciberdelincuencia, del Consejo de Europa, y considera que su implementación y aplicación práctica son cruciales en la lucha contra la ciberdelincuencia. Suiza participa en las negociaciones de un segundo protocolo adicional al Convenio, cuyo objetivo es reforzar la cooperación internacional.

A nivel bilateral, Suiza mantiene consultas políticas periódicas con los países sobre cuestiones relacionadas con la cibernética.

Suiza se unió a la Coalición para la Libertad en Línea en 2019 como su 31er miembro. Suiza cree firmemente que los mismos derechos de los que gozan las personas fuera de Internet también deben ser protegidos en línea. La Coalición para la Libertad en Línea es una iniciativa clave para reforzar el compromiso entre todas las partes interesadas con el fin de proteger los derechos humanos y las libertades fundamentales en la era de Internet. Suiza también apoya financieramente los esfuerzos de la Coalición para la Libertad en Línea.

En 2019, Suiza puso en marcha un diálogo de expertos jurídicos sobre la manera de aplicar el derecho internacional en el ciberespacio. En 2021, Suiza continuará este esfuerzo para fomentar la comprensión común de cómo se aplica el derecho

internacional, centrándose en la aplicación del derecho internacional humanitario en el ciberespacio.

En 2018, Suiza lanzó el Diálogo de Ginebra sobre el Comportamiento Responsable en el Ciberespacio, que proporciona una plataforma de múltiples interesados para debatir sobre las funciones y responsabilidades en relación con la ciberestabilidad internacional. Desde 2020, el Diálogo de Ginebra se centra en el papel de las empresas en la aplicación de las normas acordadas a nivel internacional.

El Centro Nacional de Ciberseguridad ha iniciado recientemente un proceso interinstitucional orientado a formular un enfoque pangubernamental para divulgar de manera coordinada y responsable las vulnerabilidades cibernéticas identificadas recientemente. Este proceso permite que los investigadores que detecten una vulnerabilidad en el *hardware*, el *software* y los servicios digitales la notifiquen al Centro. El objetivo de la divulgación es mitigar la vulnerabilidad (por ejemplo, aplicar un parche) antes de que la vulnerabilidad pueda ser explotada con fines malintencionados.

Suiza participa en una serie de ejercicios nacionales e internacionales, como el ejercicio Locked Shields (Escudos Trabados), con el fin de poner a prueba las capacidades nacionales, los procedimientos y los procesos de toma de decisiones.

Suiza es miembro fundador del Foro Mundial de Competencia Cibernética y apoya varios proyectos de fomento de la capacidad en el ámbito cibernético. Suiza también apoya financieramente las iniciativas destinadas a reforzar la capacidad de los diplomáticos, así como de los representantes no gubernamentales, para participar y contribuir a los procesos pertinentes de las Naciones Unidas en materia de ciberestabilidad internacional.

Turquía

[Original: inglés]
[31 de mayo de 2021]

La tecnología de la información y las comunicaciones (TIC) se ha convertido en parte esencial de la sociedad y la economía. Estas tecnologías se utilizan en una amplia red que incluye los sectores público y privado, la infraestructura crítica y las personas, y se han difundido en Turquía y en el mundo. Como resultado de ello, las TIC desempeñan un papel importante en el crecimiento y el desarrollo sostenibles. Sin embargo, cuanto más utilizamos la tecnología, más dependemos de ella y somos más vulnerables a los riesgos que conlleva. Las personas, las empresas, las infraestructuras críticas y los Estados se enfrentan a graves problemas debido a las ciberamenazas.

Turquía 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 Turquía. 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. Turquía ha desarrollado su estrategia y plan de acción nacionales de ciberseguridad 2020-2023 con la participación de todas las partes interesadas en grupos de estudio coordinados por el Ministerio de Transporte e Infraestructura.

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

- Protección y aumento de la resiliencia de las infraestructuras críticas
- Fomento de la capacidad nacional
- Red de ciberseguridad orgánica
- La seguridad de las tecnologías de nueva generación (Internet de las cosas, 5G, computación en la nube, etc.)
- 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

Además, el Equipo Nacional de Respuesta a Emergencias Informáticas, que forma parte de la Autoridad de Tecnologías de la Información y las Comunicaciones, ha coordinado la respuesta a incidentes cibernéticos en Turquía 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 relacionadas con la ciberseguridad del Equipo Nacional de Respuesta a Emergencias Informáticas son:

- Fomento de la capacidad en el ámbito cibernético
- Medidas tecnológicas
- Recopilación y difusión de información sobre amenazas
- Protección de las infraestructuras vitales

En el contexto de la mejora de la ciberseguridad nacional, desde 2013 se han establecido también 14 equipos sectoriales de respuesta a emergencias informáticas para sectores o infraestructuras críticos (como la energía, la salud, la banca y las finanzas, la gestión del agua, las comunicaciones electrónicas y los servicios públicos críticos) y 1.803 equipos institucionales de respuesta a emergencias informáticas. Todos los equipos de respuesta a emergencias informáticas operan de manera ininterrumpida bajo la coordinación del equipo nacional con el fin de mitigar los riesgos cibernéticos y luchar contra las ciberamenazas. El Equipo Nacional de Respuesta a Emergencias Informáticas utiliza herramientas de detección y prevención para la supervisión, y herramientas de notificación para compartir información con las partes pertinentes. El Equipo Nacional de Respuesta a Emergencias Informáticas desarrolló la plataforma de intercambio de información para todos los equipos de respuesta a emergencias informáticas de Turquía con el fin de distribuir alarmas, avisos y notificaciones de seguridad, lo que proporciona un canal de comunicación eficiente y seguro.

El Equipo Nacional de Respuesta a Emergencias Informáticas organiza y apoya cursos de capacitación, campamentos de verano y concursos sobre ciberseguridad abiertos a varias comunidades. Además, el equipo nacional imparte capacitación a los equipos de respuesta a emergencias informáticas sobre temas como análisis de programas maliciosos y análisis de registros. El equipo nacional ha capacitado a más de 5.000 personas en diferentes áreas de la ciberseguridad durante los últimos cuatro años.

Además, la Academia creada en el seno de la Autoridad de las Tecnologías de la Información y las Comunicaciones ofrece formación en línea abierta al público sobre ciberseguridad y otras áreas relacionadas, con el fin de contribuir a aumentar los conocimientos de los recursos humanos de Turquía. El contenido de la formación

está disponible en el portal oficial de la Academia en Internet (www.btkakademi.gov.tr/portal).

Varias organizaciones, instituciones, universidades, organizaciones no gubernamentales y entidades del sector privado de Turquía también organizan seminarios, conferencias y capacitación en todo el país sobre ciberseguridad, la protección de infraestructura crítica y otros temas conexos.

Entre las actividades de sensibilización se encuentra el Día de la Internet Segura, que se celebra anualmente y cuyo principal objetivo es el uso consciente y seguro de Internet. Existen una línea de ayuda por Internet y un sitio web seguro, donde las familias pueden encontrar consejos para el uso eficiente de Internet, a los que el público puede acceder en el portal oficial sobre Internet segura (https://www.guvenlinet.org.tr/).

Turquía también adopta medidas para contrarrestar el aumento de los riesgos de seguridad digital para garantizar la ciberseguridad y toma medidas en el ámbito de 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 Nacional 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 las infraestructuras críticas 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 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

Turquía ha desempeñado un papel importante 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, Turquía considera importante el intercambio de información con diferentes países y organizaciones en una amplia gama de esferas. El Equipo Nacional de Respuesta a Emergencias Cibernéticas es miembro del Foro de Equipos de Seguridad y Respuesta a Incidentes, el servicio Trusted Introducer, la Unión Internacional de Telecomunicaciones (UIT), la Plataforma Multinacional de Intercambio de Información sobre Programas Maliciosos de la Organización del Tratado del Atlántico Norte (OTAN), la Alianza de Ciberseguridad para el Progreso Mutuo y el Equipo de Respuesta a Emergencias Informáticas de la Organización de la Conferencia Islámica. Turquía también ha participado en el Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN en calidad de país patrocinador desde noviembre de 2015. Además, existe una cooperación bilateral y multilateral en materia de ciberseguridad, como los memorandos de entendimiento con muchos países. Asimismo, Turquía participa y contribuye activamente 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, el Consejo de Cooperación de los Estados de Habla Túrquica 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 realizados en los planos nacional e internacional contribuyen a fortalecer el ciberespacio y a poner a prueba las medidas que deben adoptarse contra posibles ciberamenazas. Desde 2011, el Ministerio de Transporte e Infraestructura ha organizado cuatro ejercicios de seguridad cibernética nacionales y dos internacionales. Más recientemente, el 19 de diciembre de 2019, el Ministerio de Transporte e Infraestructura y la Autoridad de las Tecnologías de la Información y las Comunicaciones organizaron conjuntamente en Ankara el ejercicio de seguridad cibernética internacional Cyber Shield 2019, que recibió el apoyo de la UIT y la Alianza de Seguridad Cibernética para el Progreso Mutuo. Además, Turquía participa en ejercicios internacionales de ciberseguridad y contribuye a su realización, como el ejercicio Locked Shields (Escudos Trabados) de la OTAN, la Coalición Cibernética de la OTAN y el Ejercicio de Gestión de Crisis de la OTAN. Al igual que 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.

La paz y la seguridad internacionales en el ciberespacio requieren nuevos estudios basados en una mayor cooperación internacional. Puede verse claramente que el derecho internacional y las normas y reglas enunciadas en los informes de los Grupos de Expertos Gubernamentales, los Grupos de Trabajo de Composición Abierta y en estudios conexos contribuyen a un ciberespacio más seguro.

Además, la mejora de la colaboración y el apoyo a los mecanismos de intercambio de información son fundamentales para luchar contra las ciberamenazas y se les ha de dar la debida importancia.

Además, Turquía 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 la necesidad de una cooperación internacional eficaz. Turquía toma las medidas necesarias con determinación para garantizar la consecución de estos objetivos, y el fortalecimiento de la ciberseguridad a nivel nacional e internacional seguirá siendo una de sus principales prioridades.

Ucrania

[Original: inglés]
[31 de mayo de 2021]

El análisis de la información disponible muestra que, en las condiciones de la guerra “híbrida” contra nuestro Estado, una de las principales amenazas a la seguridad nacional son las destructivas operaciones especiales psicológicas y de información de la Federación de Rusia, destinadas a socavar el orden constitucional, violar la soberanía y la integridad territorial de Ucrania y agravar la situación sociopolítica y socioeconómica de nuestro país. La difusión intencionada de desinformación e información falsa, junto con la agresión armada, se ha convertido en una amenaza urgente no solo para Ucrania, sino también para todo el mundo, ya que afecta a la conciencia de los ciudadanos de otros países, crea una imagen distorsionada de Ucrania y forma una opinión pública que es beneficiosa solo para Rusia.

El Estado agresor está tomando cada vez más medidas destinadas a reducir el nivel de seguridad de la información de nuestro Estado, creando mecanismos para influir en las instituciones estatales y el espacio de la información con el fin de fortalecer su propia posición, formando una opinión extranjera favorable y ejerciendo presión sobre las instituciones estatales ucranianas para que tomen decisiones a su favor. Para ello, se realiza una promoción en el espacio informativo y mediático ucraniano, de forma sistemática, y en Internet, en particular a través de las redes

sociales, los sistemas de envío de mensajes, los recursos electrónicos y los productos informativos especialmente preparados, sobre todo con carácter de desinformación.

Para implementar esta influencia informativa negativa en nuestro país, la Federación de Rusia ha creado un poderoso sistema de promoción de contenidos propagandísticos, que incluye una red de plataformas informativas (blogs, sitios), medios de comunicación y recursos de Internet controlados, agregadores y concentradores de noticias, blogueros y líderes de opinión para publicar contenidos, agencias de noticias y empresas de relaciones públicas para mostrar mensajes propagandísticos en los principales canales de noticias. También está muy extendido el uso por parte de Rusia de redes de *bots* para difundir rápidamente información errónea y mensajes contrarios a Ucrania con el objetivo de manipular la conciencia de las masas. Los sujetos clave del espacio informativo utilizado por la parte rusa para difundir información errónea son las principales redes sociales del mundo (Facebook, Instagram, Twitter), cuyo rápido crecimiento de audiencia se ha producido debido a la prohibición en Ucrania de las redes sociales rusas VKontakte y Odnoklassniki. Existe una tendencia a reorientar a los usuarios del segmento ucraniano de Internet hacia el uso generalizado de servicios de mensajería (Telegram, WhatsApp, Viber, etc.), debido a la posibilidad de mantener el anonimato, la eficacia de la colocación y posterior distribución masiva de contenidos, y los altos niveles de interactividad y retroalimentación.

También se utilizan servicios de alojamiento de vídeos (YouTube, Yandex.Video, RuTube, Video@Mail.Ru) para difundir información errónea, ya que las empresas propietarias de los servicios de alojamiento de fotos y vídeos operan de acuerdo con las leyes de los países en cuyo territorio se encuentran. Los propagandistas rusos se sirven de ello para crear y publicar en estas plataformas web contenidos que suponen una amenaza para la seguridad de la información de Ucrania. Dado que dichos mensajes tienen su origen en alojamientos en los Estados Unidos y Europa, el contenido se distribuye libremente en Internet.

Además, el país agresor se esfuerza por desarrollar constantemente una red de recursos informativos controlados. En particular, las administraciones de ocupación en los territorios de nuestro Estado ocupados temporalmente están tomando medidas sistemáticas destinadas a crear nuevas plataformas de información, aumentar el número de canales de televisión y ampliar la zona de cobertura de la difusión televisiva y radiofónica, incluso en los territorios controlados por las autoridades ucranianas. Unos potentes equipos de retransmisión instalados por las autoridades de ocupación rusas, se utilizan, además de para distribuir contenidos contrarios a Ucrania, para suprimir la señal de la televisión y la radio nacionales, difundiendo el llamado “ruido blanco” en las frecuencias que utiliza la parte ucraniana para transmitir información objetiva a los residentes de los territorios temporalmente ocupados. Esto es especialmente relevante teniendo en cuenta que la señal por satélite de los canales de televisión de los mayores grupos mediáticos del país (Inter Media Group, StarLightMedia, Media Group Ukraine, 1 + 1) está codificada y que la cobertura en el territorio de Ucrania de la televisión y la radio nacionales transmitidas en norma digital es insatisfactoria. Como resultado, los residentes de las zonas fronterizas de Ucrania están bajo la constante influencia de contenidos destructivos de los principales canales de propaganda de la Federación de Rusia. Otro factor negativo, que complica la entrega de contenidos localizados a los residentes de los territorios de Ucrania temporalmente ocupados, es la actuación de los operadores y proveedores de los territorios temporalmente ocupados, que limitan el acceso de la población local al segmento ucraniano de Internet. Así, en violación de la legislación europea, el registro de las direcciones IP para el funcionamiento de los llamados proveedores de Internet en Crimea y en las zonas ocupadas de Dombás es proporcionado por la organización sin fines de lucro Centro de Coordinación de Redes

IP Europeas (Países Bajos). A fin de adecuar las actividades de esta organización a la legislación vigente de Ucrania, el Ministerio de Relaciones Exteriores de Ucrania y la Embajada de Ucrania en el Reino de los Países Bajos están adoptando las medidas oportunas a nivel interestatal.

También hay casos en los que la Federación de Rusia utiliza los servicios de Apple y Google para difundir información errónea con el fin de manipular a los usuarios del segmento ucraniano de Internet. En particular, en la App Store y en el Play Market hay aplicaciones móviles desarrolladas por personas jurídicas y físicas que han sido objeto de medidas económicas especiales y otras medidas restrictivas (sanciones) de conformidad con la Decisión del Consejo Nacional de Seguridad y Defensa de 14 de mayo de 2020 sobre la aplicación, anulación y modificación de las medidas económicas especiales personales y otras medidas restrictivas (sanciones), promulgada por el Decreto núm. 184/2020 del Presidente de Ucrania de 14 de mayo de 2020. Estos productos de *software*, por sus funciones, tienen la capacidad técnica de proporcionar acceso a los recursos web prohibidos en Ucrania.

A pesar de todos los esfuerzos de nuestro Estado por reforzar la seguridad de la información y bloquear la difusión de la información errónea, como una de las mayores amenazas en la esfera de la información, es urgente ayudar a la comunidad mundial y a las instituciones internacionales a contrarrestar adecuadamente la agresión informativa de la Federación de Rusia, no solo contra Ucrania, sino también en relación con otros países, desde cuya posición lleva a cabo acciones de influencia destructiva en el espacio de la información.

Hasta hace poco, la influencia informativa destructiva de la Federación de Rusia y sus intentos de interferir en los asuntos internos de nuestro Estado y de imponer sus condiciones en la aplicación de la cooperación internacional y los procesos internos se llevaban a cabo a través de los partidos y movimientos políticos ucranianos afiliados, la financiación encubierta directa de las instituciones cívicas y las entidades económicas que operan en el territorio de nuestro Estado, fuertes presiones a través de la agresión militar en el este de Ucrania o el bloqueo del apoyo internacional y de la adhesión de Ucrania a la Unión Europea y a la Organización del Tratado del Atlántico Norte (OTAN), y la realización de campañas, operaciones y acciones de información a través de recursos informativos controlados.

Sin embargo, existe una tendencia progresiva según la cual la Federación de Rusia está reorientando las siguientes fases de la estrategia de la llamada “guerra de la información” contra Ucrania, para ocultar su participación en la organización y ejecución de medidas destructivas contra nuestro Estado, aplicándolas desde la posición de los llamados “terceros” países. Por un lado, esto se produce debido a las sanciones económicas impuestas por la Unión Europea y los Estados Unidos contra la Federación de Rusia por la injerencia en los asuntos internos de Ucrania, la anexión de la República Autónoma de Crimea y el conflicto armado en los territorios ocupados temporalmente de las regiones de Donetsk y Luhansk. Por otro, también se debe a las medidas tomadas por la parte ucraniana para combatir la influencia destructiva del país agresor sobre el espacio informativo ucraniano y la conciencia de los ciudadanos, mitigar las consecuencias negativas de los mensajes difundidos y aumentar el nivel de patriotismo y conciencia de la población de nuestro Estado.

En particular, aumentan las acciones de influencia informativa y las injerencias en los asuntos internos de Ucrania. La Federación de Rusia está llevando a cabo actividades subversivas y de inteligencia dirigidas a los Estados miembros de la OTAN y de la Unión Europea, consistentes en la creación y financiación de grupos de presión en favor de los intereses rusos dentro de las autoridades y la administración estatal y local, los partidos y movimientos políticos, la comunidad de expertos y blogueros, los grupos de reflexión, las empresas de publicidad y consultoría, los

donantes, las organizaciones no gubernamentales y los líderes de opinión pública, así como mediante la creación de medios de comunicación, recursos de Internet y empresas de relaciones públicas controlados.

Mediante los políticos europeos prorrusos de las células del llamado “mundo ruso” en la Unión Europea, la Federación de Rusia está tratando de legalizar e imponer a la comunidad mundial la idea de que el plebiscito de Crimea fue legítimo, justificar su agresión armada contra Ucrania y, en consecuencia, lograr el levantamiento de las sanciones antirrusas y su regreso a la comunidad política mundial. Actualmente, hay ramas prorrusas activas en algunos Estados europeos. La mayoría de los representantes de estas fuerzas políticas, al ser miembros de grupos de presión que abogan por los intereses del país agresor tanto dentro como fuera de su país, propagan opiniones prorrusas, difunden narrativas rusas y adoptan medidas informativas que amenazan los intereses nacionales de Ucrania.

La reorientación de la Federación de Rusia hacia la organización y realización desde “terceros” países de operaciones especiales de información y acciones de influencia informativa destructiva se manifiesta fomentando contradicciones históricas y reivindicaciones territoriales de otros Estados hacia Ucrania y provocando manifestaciones separatistas y en pro de la autonomía entre las minorías nacionales de Ucrania. Por un lado, esto complica las relaciones entre nuestro Estado y los países vecinos, desde cuya posición la Federación de Rusia lleva a cabo tales actividades destructivas, y por otro lado, se convierte en un motivo para que estos países declaren sus reclamaciones territoriales sobre ciertas tierras ucranianas. Al mismo tiempo, al distanciarse oficialmente de este proceso, Rusia evita las acusaciones directas de Ucrania y de la comunidad mundial de injerencia en los asuntos internos de nuestro Estado, y amenaza directamente las relaciones de buena vecindad de Ucrania con otros Estados, para conformar posiciones de influencia sobre la situación política interna de Ucrania.

En vista de lo anterior, Ucrania seguirá adoptando medidas amplias para garantizar un comportamiento responsable en el ciberespacio en el contexto de la seguridad internacional, al tiempo que pide el apoyo de la comunidad mundial y esfuerzos conjuntos para contrarrestar adecuadamente la guerra “híbrida” de la Federación de Rusia.

Con el fin de garantizar la aplicación de la reforma de la legislación sobre la firma digital electrónica mediante la armonización con las disposiciones del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, la Rada Suprema de Ucrania aprobó el 5 de octubre de 2017 la Ley núm. 2155-VIII sobre Servicios Electrónicos de Confianza, que entró en vigor el 7 de noviembre de 2018.

El objetivo principal es introducir en Ucrania los modelos y principios para la prestación de servicios electrónicos de confianza utilizados en la Unión Europea, sin destruir el sistema de interacción entre las partes en el ámbito de la firma digital electrónica que se ha desarrollado en Ucrania. La Ley define los principios jurídicos y organizativos de la prestación de servicios electrónicos de confianza, incluidos los servicios transfronterizos, los derechos y obligaciones de los sujetos de las relaciones en el ámbito de los servicios electrónicos de confianza, el procedimiento de supervisión (control) estatal del cumplimiento de la legislación en el ámbito de los servicios electrónicos de confianza y los principios jurídicos y organizativos de la identificación electrónica. En desarrollo de las disposiciones de la Ley núm. 2155-VIII, el Consejo de Ministros de Ucrania adoptó una serie de resoluciones:

- Núm. 749 sobre la aprobación del procedimiento para el uso de los servicios electrónicos de confianza en las autoridades públicas, los gobiernos locales y las empresas, instituciones y organizaciones de propiedad estatal, adoptada por el Consejo de Ministros de Ucrania el 19 de septiembre de 2018.
- Núm. 775 sobre la aprobación de los requisitos obligatorios con respecto a la lista de referencia, adoptada por el Consejo de Ministros de Ucrania el 26 de septiembre de 2018.
- Núm. 821 sobre la aprobación del procedimiento de almacenamiento de la información documental y su transferencia al órgano central de gestión en caso de cese de las actividades de un emisor cualificado de servicios electrónicos de confianza, adoptada por el Consejo de Ministros de Ucrania el 10 de octubre de 2018.
- Núm. 992 sobre la aprobación de los requisitos en el ámbito de los servicios electrónicos de confianza y el procedimiento para las inspecciones del cumplimiento de los requisitos de la legislación en el ámbito de los servicios electrónicos de confianza, adoptada por el Consejo de Ministros de Ucrania el 7 de noviembre de 2018.
- Núm. 1215 sobre la aprobación de los procedimientos de evaluación de la conformidad en el ámbito de los servicios electrónicos de confianza, adoptada por el Consejo de Ministros de Ucrania el 18 de diciembre de 2018.
- Núm. 60 sobre la aprobación del procedimiento de reconocimiento mutuo de los certificados de clave pública ucranianos y extranjeros, de las firmas electrónicas y del uso del sistema de información y telecomunicaciones del órgano central encargado de garantizar el reconocimiento en Ucrania de los servicios electrónicos de confianza y de los certificados de clave pública extranjeros utilizados durante la prestación de servicios electrónicos con efectos legales en el proceso de interacción entre sujetos de diferentes Estados, adoptada por el Consejo de Ministros de Ucrania el 23 de enero de 2019.

La Administración de Comunicaciones Especiales y Protección de la Información de Ucrania, en cumplimiento de los requisitos del artículo 8 de la Ley, aprobó mediante orden de fecha 14 de mayo de 2020 los requisitos para la seguridad y protección de la información sobre los proveedores calificados de servicios de referencia electrónicos y sus puntos de registro separados (registrados en el Ministerio de Justicia de Ucrania el 16 de julio de 2020), que detallan y especifican la aplicación de la Ley y los requisitos en el ámbito de los servicios de confianza electrónicos, aprobados por el Consejo de Ministros de Ucrania el 7 de noviembre de 2018 mediante la resolución núm. 992, para garantizar la seguridad y protección de la información sobre los proveedores de servicios electrónicos de confianza y los puntos de registro separados.

En la actualidad, Ucrania está adoptando medidas encaminadas al reconocimiento mutuo de los servicios electrónicos de confianza en el marco del Acuerdo de Asociación entre Ucrania y la Unión Europea y como resultado de los acuerdos alcanzados entre Ucrania y la Unión Europea durante la 22ª cumbre entre la Unión Europea y Ucrania.

Al mismo tiempo, es necesario revisar algunas disposiciones de la Ley a fin de adecuarlas en la medida de lo posible con lo dispuesto en el Reglamento (UE) núm. 910/2014, en particular en lo que se refiere al establecimiento de la normativa estatal en el ámbito de la identificación electrónica, a la necesidad de contar con firmas y sellos electrónicos mejorados y a la aclaración de los requisitos de las firmas o sellos electrónicos cualificados. El Ministerio de Transformación Digital y la Administración de Comunicaciones Especiales y Protección de la Información de

Ucrania han elaborado un proyecto de ley que está siendo examinado por el Consejo de Ministros de Ucrania.

Además, mediante la resolución núm. 24 de 13 de enero de 2021, el Consejo de Ministros de Ucrania modificó el apartado 4 del Reglamento sobre la Administración del Servicio Estatal de Comunicaciones Especiales y Protección de la Información de Ucrania, que gestiona la Administración Estatal de Comunicaciones Especiales, y estableció las funciones del Organismo de Acreditación Segura instituido de conformidad con el artículo 7 sobre los acuerdos administrativos para la protección de la información de acceso restringido entre el Gobierno de Ucrania y la OTAN, ratificados por la Ley núm. 2068 de 24 de mayo de 2017.

La Administración de Comunicaciones Especiales y Protección de la Información de Ucrania, mediante el establecimiento de un procedimiento de acreditación nacional para la seguridad del sistema de comunicación e información destinado al intercambio de información de acceso restringido de la OTAN, toma medidas para aplicar la normativa de la OTAN sobre estas cuestiones.

En el marco de la promoción de la cooperación internacional y la sensibilización de los profesionales de la seguridad de la información, la Administración de Comunicaciones Especiales y Protección de la Información de Ucrania participa en conferencias internacionales de la Oficina de Asistencia Técnica e Intercambio de Información (TAIEX) de la Comisión Europea y en seminarios de FireEye.

Con el objetivo de reforzar la seguridad de la información, se está introduciendo de forma progresiva un sistema de auditoría de seguridad de la información en las instalaciones de infraestructuras críticas, como se indica a continuación:

- Formulación de requisitos para los auditores independientes de seguridad de la información en las instalaciones de infraestructuras críticas.
- Desarrollo del procedimiento de certificación o recertificación de los auditores de seguridad de la información, así como de un sistema de evaluación especial de la formación profesional de los auditores de seguridad de la información y análisis de los resultados de la auditoría independiente de seguridad de la información en los aspectos de la “auditoría” de la seguridad de la tecnología de la información relacionados con infraestructuras críticas.

Al mismo tiempo, con el fin de aplicar la política estatal en el ámbito de la protección de la información, el personal de la Administración de Comunicaciones Especiales y Protección de la Información de Ucrania lleva a cabo medidas de control nacional sobre el estado de la protección técnica en el ciberespacio de los recursos de información del Estado y la información como dispone la ley.

Además, la Administración de Comunicaciones Especiales y Protección de la Información de Ucrania ha tomado una serie de medidas para preparar y garantizar la aprobación de las siguientes leyes:

– Preparó propuestas exhaustivas para el proyecto de estrategia de ciberseguridad de Ucrania (2021-2025) de conformidad con el artículo 107 de la Constitución de Ucrania, la segunda parte del artículo 2 de la Ley sobre los Fundamentos de la Seguridad Nacional y el Decreto núm. 391/2020 del Presidente de Ucrania sobre la decisión del Consejo Nacional de Seguridad y Defensa de 14 de septiembre de 2020.

– Prestó apoyo a la adopción de la resolución núm. 518, de 19 de junio de 2019, del Consejo de Ministros de Ucrania sobre la aprobación de los requisitos generales para la ciberprotección de las infraestructuras críticas, que se inició en el marco de la formación y aplicación de la política estatal sobre la

ciberprotección de las infraestructuras de información críticas y que tenía por objeto lograr la compatibilidad con las normas pertinentes de la Unión Europea y la OTAN, así como la creación de un marco normativo y terminológico sobre la ciberseguridad y la armonización de la normativa en el ámbito de la seguridad de la información y la ciberseguridad de conformidad con las normas internacionales.

– El Consejo de Ministros de Ucrania adoptó la resolución núm. 1109 sobre algunas cuestiones de las instalaciones de infraestructuras críticas y la resolución núm. 943 sobre algunas cuestiones de las instalaciones de infraestructuras de información críticas, que se elaboraron teniendo en cuenta los requisitos de la legislación de la Unión Europea, en particular la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un alto nivel común de seguridad de las redes y los sistemas de información en la Unión, y la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

– El 11 de noviembre de 2020, el Consejo de Ministros de Ucrania adoptó la resolución núm. 1176 sobre la aprobación del procedimiento de examen del estado de la protección cibernética de la infraestructura de información crítica, los recursos de información y la información del Estado como dispone la ley, que permite la regulación de las infraestructuras de información, los recursos de información del Estado y la información cuya protección exige la ley.

El Equipo de Respuesta a Emergencias Informáticas de Ucrania adopta constantemente medidas de cooperación con equipos extranjeros para abordar cuestiones relacionadas con la superación de los efectos de los ciberataques en las infraestructuras de información críticas, analiza los datos sobre ciberincidentes, proporciona a los propietarios de instalaciones de ciberseguridad asistencia práctica para prevenir, detectar y eliminar las consecuencias de los ciberincidentes, prepara y publica recomendaciones para combatir los tipos modernos de ciberataques y ciberamenazas en su sitio web oficial y proporciona información sobre las ciberamenazas y los métodos adecuados de protección contra ellas.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[31 de mayo de 2021]

El Reino Unido acoge con satisfacción la invitación a informar al Secretario General de sus opiniones y observaciones sobre cuestiones relativas a la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, como se detalla en la resolución 75/32 de la Asamblea General. Alentamos a todos los Estados que participan en los debates relativos a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional a que aprovechen esta y otras oportunidades posteriores.

El ciberespacio no entiende de fronteras nacionales. Como ciberpotencia responsable, el Reino Unido trabajará para dar forma a los futuros marcos que rigen el ciberespacio, defendiendo las normas existentes y construyendo un consenso sobre normas positivas de comportamiento en un mundo fundamentalmente moldeado por la tecnología.

El Reino Unido reconoce que, a lo largo de la próxima década, el rápido cambio tecnológico en áreas como la inteligencia artificial, la cibernética y los datos cambiarán la forma de nuestras sociedades. Los países deben trabajar unidos para

hacer frente a los mayores retos mundiales, entre ellos promover un ciberespacio libre, abierto, pacífico y seguro y actuar como una fuerza del bien en el mundo, defendiendo la democracia y los derechos humanos en nuestras sociedades digitales.

Promoveremos la adopción y el cumplimiento de esas reglas y normas y trabajaremos de forma concertada con toda una serie de asociados e interesados para hacer valer un argumento convincente a favor de un ciberespacio que proteja a las sociedades abiertas y permita la innovación, el desarrollo y el crecimiento. También apoyaremos a los países que se enfrentan a los retos de la digitalización —mediante la creación de capacidades internacionales— a fin de que adquieran la confianza necesaria para participar en el debate internacional y aumenten sus capacidades de ciberseguridad.

El Reino Unido se congratula de la conclusión satisfactoria de los procesos concurrentes de las Naciones Unidas, 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 y el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional. El Grupo de Trabajo de Composición Abierta ha proporcionado un proceso inclusivo que representa los diversos puntos de vista de todos los Estados Miembros y otros interesados, al tiempo que creemos que el informe del Grupo de Expertos Gubernamentales proporcionará la guía detallada del marco inicial para el comportamiento responsable de los Estados en el ciberespacio que muchos Estados han solicitado.

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

El 16 de marzo de 2021 el Reino Unido publicó *Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy*[9], que describe la visión del Gobierno sobre el papel del Reino Unido en el mundo durante la próxima década y las medidas que adoptaremos hasta 2025. En ese examen se identifica la necesidad de dar forma al orden internacional a medida que este se desarrolla en las fronteras futuras, en los dominios del ciberespacio y del espacio, donde las posibilidades de actividad económica, social y militar se están expandiendo rápidamente. Participaremos activamente para garantizar una responsabilidad y una supervisión efectivas que protejan los valores democráticos, al tiempo que nos opondremos a las extralimitaciones del control estatal.

El Reino Unido también adoptará en 2021 una ciberestrategia nueva y amplia que sustituirá a la anterior estrategia nacional de ciberseguridad 2016-2021. La necesidad de un enfoque “pangubernamental” de las cuestiones cibernéticas será la base de la estrategia, tal y como se preveía en el examen integrado. En el marco de esta estrategia, nuestras acciones prioritarias serán:

- Reforzar el ciberecosistema del Reino Unido, haciendo posible un enfoque nacional de la cibernética y profundizando en la asociación entre el Gobierno, el mundo académico y la industria.
- Construir un Reino Unido digital resiliente y próspero, donde los ciudadanos se sientan seguros en línea y confíen en que sus datos están protegidos.

[9] www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

- Tomar la delantera en las tecnologías vitales para la potencia cibernética, como los microprocesadores, el diseño de sistemas seguros, las tecnologías cuánticas y las nuevas formas de transmisión de datos.
- Promover un ciberespacio libre, abierto, pacífico y seguro, trabajando con otros Gobiernos y con la industria y aprovechando el liderazgo intelectual del Reino Unido en materia de ciberseguridad.
- Detectar, perturbar y disuadir a nuestros adversarios.

A través de estas estrategias, trabajaremos con otros Gobiernos y en asociación con la industria para garantizar que el ciberespacio se rija por reglas y normas que mejoren la seguridad colectiva, promuevan los valores democráticos y apoyen el crecimiento económico mundial, y actúen contra la propagación del autoritarismo digital. El Reino Unido defenderá el estado de derecho en el ciberespacio, dando ejemplo del comportamiento responsable de los Estados y conformando las mejores prácticas internacionales, así como incentivando el cumplimiento, desalentando los ataques y haciendo que otros rindan cuentas por el comportamiento irresponsable de los Estados. Cuando sea necesario, daremos forma a las normas para que las herramientas cibernéticas ofensivas se desarrollen y utilicen de forma responsable y de acuerdo con el derecho internacional.

Además haremos lo siguiente:

- Proteger una Internet mundial accesible e interoperable para las generaciones futuras.
- Garantizar que los derechos humanos estén protegidos en línea, como lo están fuera de Internet.
- Garantizar que la transparencia y la responsabilidad se integren desde el principio en el diseño y el despliegue de las nuevas tecnologías.
- Defender el flujo internacional de datos, permitiendo un intercambio seguro, fiable e interoperable a través de las fronteras, manteniendo al mismo tiempo las normas de protección de datos.

El Reino Unido considera que la ciberdiplomacia es un elemento crítico de su liderazgo cibernético, con una red de funcionarios que se extiende por 6 continentes. Además de nuestros programas de fomento de la capacidad en ciberseguridad, hemos iniciado diálogos intergubernamentales con 20 países. A través de esos programas, seguiremos ampliando las asociaciones para reforzar los argumentos en favor de un ciberespacio libre, abierto, pacífico y seguro, y para responder a las ciberactividades malintencionadas dirigidas por los Estados y desalentarlas.

Seguimos participando en una amplia gama de foros mundiales y regionales dedicados a los debates sobre ciberseguridad, entre ellos el Grupo de Trabajo de Composición Abierta de las Naciones Unidas y el Grupo de Expertos Gubernamentales de las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Unión Internacional de Telecomunicaciones y el Foro Mundial de Competencia Cibernética.

El Reino Unido puede atribuir actos cibernéticos malintencionados a los Estados, y de hecho lo hace, cuando cree que redunda en su interés, y en aras de su compromiso con la claridad y la estabilidad en el ciberespacio. Seguimos considerando que la decisión de atribuir a un Estado una ciberactividad malintencionada, y sobre todo de hacer pública esa atribución, es en última instancia una decisión política de los Estados. Las declaraciones y otra información relevante están disponibles en línea en www.gov.uk y www.ncsc.gov.uk.

En 2020, el Reino Unido creó la Fuerza Cibernética Nacional. Somos uno de los países que han confirmado públicamente que están desarrollando estas capacidades. La Fuerza Cibernética Nacional lleva a cabo ciberoperaciones ofensivas específicas y responsables a fin de apoyar las prioridades de seguridad nacional del Reino Unido, reuniendo las capacidades de defensa e inteligencia. Se emplea en combinación con las capacidades diplomáticas, económicas, políticas y militares; algunos posibles ejemplos de ciberoperaciones son:

- Interferir un teléfono móvil para impedir que un terrorista pueda comunicarse con sus contactos.
- Ayudar a evitar que el ciberespacio se utilice como plataforma mundial para cometer delitos graves, como el fraude y los abusos sexuales de niños.
- Mantener a los aviones militares del Reino Unido a salvo de ataques con sistemas de armas.

El Reino Unido se compromete a utilizar sus cibercapacidades de forma responsable, de acuerdo con la legislación del Reino Unido y el derecho internacional. Las ciberoperaciones pasadas y futuras han operado y continuarán operando bajo las leyes existentes, incluyendo la Ley de Servicios de Inteligencia de 1994 y la Ley de Facultades de Investigación de 2016. Esto garantiza que las ciberoperaciones del Reino Unido sean responsables, específicas y proporcionadas.

Todos los Estados Miembros han acordado que promover el uso de las tecnologías de la información y las comunicaciones (TIC) con fines pacíficos redunda en interés de todos los Estados. El Reino Unido vuelve a confirmar que las TIC no son en sí mismas una “amenaza”. Más bien, la amenaza o el riesgo surgen cuando los Estados (u otros actores) optan por utilizar las TIC o se percibe que lo hacen “con fines incompatibles con la paz y la seguridad internacionales”. En este contexto, ahondar en el debate sobre cómo entienden los Estados que se aplica el derecho internacional cuando actúan en el ciberespacio es un paso práctico para aumentar la transparencia, la previsibilidad y la estabilidad.

La información más reciente sobre los planteamientos del Reino Unido en materia de ciberseguridad, incluso en lo que respecta a la cooperación internacional, puede encontrarse en línea en www.gov.uk/government/cyber-security y www.ncsc.gov.uk.

Contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales

El Reino Unido se congratula de que en ambos procesos los Estados Miembros hayan reafirmado los tres anteriores informes de los Grupos de Expertos Gubernamentales aprobados por consenso de 2010, 2013 y 2015, en los que se confirmó que el derecho internacional se aplica al ciberespacio y se estableció un marco de comportamiento responsable de los Estados consistente en un conjunto de normas voluntarias y no vinculantes y de medidas de fomento de la confianza, apuntaladas por la creación de capacidades. Los nuevos informes de 2021 serán una importante contribución al acervo.

El Reino Unido considera que la correcta aplicación, en su totalidad y por todos los Estados, del marco esbozado en los informes existentes proporciona un punto de partida práctico para nuestros esfuerzos por aumentar la estabilidad en el ciberespacio. La universalización y puesta en marcha de las evaluaciones y recomendaciones acumuladas sería un paso práctico. Por lo tanto, se necesitan enfoques prácticos y orientados a la acción.

Amenazas existentes y nuevas amenazas

En cuanto a las tendencias en desarrollo, durante la pandemia de enfermedad por coronavirus (COVID-19), los atacantes aprovecharon la crisis a la hora de seleccionar sus objetivos, entre los que se encontraban hospitales y otras infraestructuras críticas relacionadas con la salud. Los agentes malintencionados eligieron activamente como blanco a las organizaciones que participaban en las respuestas nacionales e internacionales a la COVID-19. Entre esas organizaciones figuran organismos sanitarios, empresas farmacéuticas, instituciones académicas, organizaciones de investigación médica y autoridades locales. Estos agentes suelen atacar a las organizaciones para recopilar información personal masiva, propiedad intelectual e información de inteligencia que se ajusta a las prioridades nacionales.

El uso de programas secuestradores se ha convertido en uno de los tipos de incidentes más frecuentes y perturbadores de los que se ocupa el Centro Nacional de Ciberseguridad del Reino Unido. En el examen anual de 2020[10], observamos que el Centro gestionó más del triple de incidentes que el año anterior. En el Reino Unido también se produjo un aumento de los ataques con programas secuestradores que afectaron al sector educativo en un momento en que las instituciones se esforzaban por gestionar los procedimientos de aprendizaje, admisión y exámenes en línea. Los atacantes están aumentando la presión, ya que amenazan con filtrar públicamente los datos robados cuando las víctimas se resisten a pagar el rescate. También hemos visto que los ataques se volvían más sofisticados y los atacantes permanecían en una red durante un tiempo y buscaban los datos más valiosos para cifrarlos, así como cualquier copia de seguridad en línea para obstaculizar la recuperación.

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

El Reino Unido afirma que todo el derecho internacional vigente, incluido el respeto por los derechos humanos y las libertades fundamentales y la aplicación del derecho internacional humanitario a las operaciones cibernéticas en los conflictos armados, forma parte de nuestro compromiso común de comportarnos de forma responsable en el ciberespacio. El derecho internacional se aplica en su totalidad de la misma manera que se aplica a las actividades del Estado fuera de Internet.

En este sentido, acogemos con satisfacción el llamamiento del Comité Internacional de la Cruz Roja para que todos los Estados reafirmen que el derecho internacional humanitario se aplica a la realización de ciberoperaciones durante los conflictos armados. Cuando los Estados participan en ciberoperaciones, estas se rigen por el derecho internacional de la misma forma que las actividades en cualquier otro ámbito. La aplicación del derecho internacional humanitario a las ciberoperaciones en los conflictos armados proporciona tanto protección como claridad. No fomenta este tipo de conflictos y garantiza que se aplique el conjunto de principios y normas existentes que tratan de minimizar las consecuencias humanitarias de los conflictos.

Sin embargo, creemos que todos debemos ir más allá como Estados individuales y establecer nuestra propia comprensión de cómo se aplica el derecho internacional al ciberespacio. El Reino Unido lo hizo en 2018 cuando el ex-fiscal general Jeremy Wright, Abogado de la Reina y Miembro del Parlamento, expuso la posición del Reino Unido sobre la aplicación del derecho internacional al ciberespacio. Era la primera vez que un ministro del Gobierno dejaba constancia de la opinión del Reino Unido.

También reconocemos la necesidad de crear capacidad en relación con el derecho internacional, mediante, entre otras cosas, posibles ejercicios relacionados

[10] www.ncsc.gov.uk/news/annual-review-2020.

con nuestra comprensión de la aplicación del derecho internacional. El fomento de la capacidad en este ámbito podría suponer una diferencia tangible en la capacidad de los Estados para desarrollar sus propias posiciones y defender sus intereses nacionales en futuras negociaciones, así como para garantizar que con ello no ahondamos inadvertidamente la brecha digital.

Normas, reglas y principios para el comportamiento responsable de los Estados

En septiembre de 2019, el Reino Unido presentó al Grupo de Trabajo de Composición Abierta un documento oficioso sobre las actividades encaminadas a aplicar las normas sobre la conducta responsable de los Estados en el ciberespacio, acordadas en los informes del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2010, 2013 y 2015[11]. Este sigue siendo una guía eficaz para las actividades del Reino Unido encaminadas a aplicar las normas sobre la conducta responsable de los Estados. Acogimos con satisfacción la presentación por parte del Grupo Asesor de Múltiples Interesados sobre Cuestiones Cibernéticas del Reino Unido de un documento complementario[12], que ofrece sugerencias sobre cómo los interesados pueden contribuir a la aplicación de las normas en apoyo de los Estados.

El Reino Unido cree que, para que las normas surtan efecto, es necesario cumplirlas. Los factores clave en su aplicación son los siguientes:

- Toma de conciencia entre los Gobiernos y las comunidades interesadas para ayudar a desarrollar una comprensión compartida del valor de las normas y promover su adopción.
- Recursos para apoyar la aplicación. La aplicación de las normas puede y debe ser un elemento de cualquier estrategia nacional de ciberseguridad. En 2019, solo el 40 % de los Estados tenían una estrategia de este tipo. El Reino Unido sigue apoyando a una serie de Estados en el desarrollo de su cibercapacidad nacional.
- Disponibilidad de orientaciones sobre las mejores prácticas en materia de aplicación. El Reino Unido cree que el informe del Grupo de Expertos Gubernamentales proporcionará una guía detallada del marco inicial para el comportamiento responsable del Estado en el ciberespacio que muchos Estados han solicitado. El documento oficioso y el documento complementario a los que se ha hecho referencia también contribuyen a la creación de mejores prácticas en este ámbito.

Medidas de fomento de la confianza

El Reino Unido considera que los Estados deberían centrarse en hacer operativas las medidas de fomento de la confianza existentes en lugar de desarrollar otras nuevas. Las organizaciones regionales son vehículos importantes en la universalización y puesta en práctica de las recomendaciones de los anteriores Grupos de Expertos Gubernamentales, junto con el sector privado, el mundo académico y las organizaciones de la sociedad civil. Sin embargo, la puesta en práctica de las medidas de fomento de la confianza sigue siendo limitada, lo que deja una importante laguna en la eficacia potencial de nuestro marco.

El Reino Unido participa activamente en el Grupo de Trabajo Oficioso sobre Medidas de Fomento de la Confianza Cibernética de la OSCE. Hemos adoptado la

[11] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf.

[12] www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf.

medida de fomento de la confianza núm. 5 de la OSCE, relativa al fomento de la capacidad, y nos hemos comprometido a apoyar su puesta en marcha entre los Estados de la OSCE. En 2019 organizamos un debate basado en un escenario cibernético con el fin de practicar la aplicación y la comprensión de las medidas de fomento de la confianza entre 40 Estados miembros. En 2020 y 2021, el Reino Unido ha presidido el Comité de Seguridad de la OSCE, aprovechando su papel para acoger dos eventos centrados en la cibernética.

Fomento de la capacidad

El Reino Unido es uno de los principales donantes bilaterales para el fomento de la capacidad cibernética. Consideramos que las Naciones Unidas pueden utilizar su poder de convocatoria para dar más visibilidad al fomento de la capacidad en materia de ciberseguridad y fomentar las buenas prácticas coordinadas. Para maximizar la eficiencia y la eficacia, será importante involucrar a todas las partes interesadas y evitar la duplicación del trabajo existente. El Foro Mundial de Competencia Cibernética ya es un mecanismo eficaz de coordinación para el fomento de la capacidad. Las herramientas independientes de revisión de la capacidad, las guías de mejores prácticas y las organizaciones, como el Foro de Equipos de Seguridad y Respuesta a Incidentes de la comunidad de equipos de respuesta a incidentes de ciberseguridad, también contribuyen de forma importante a este objetivo.

Durante el período 2019-2021, el Reino Unido fue patrocinador de la beca Women in International Security and Cyberspace. Estamos especialmente orgullosos de haber contribuido, a través de este programa, a aumentar la participación de las mujeres en el Grupo de Trabajo de Composición Abierta.

Diálogo institucional periódico

El Reino Unido patrocina la propuesta de un programa de acción que facilite un diálogo institucional regular e inclusivo en las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio. Apoyamos que se siga trabajando para elaborar y establecer esta propuesta.

III. Respuestas recibidas de organizaciones intergubernamentales

Unión Europea

[Original: inglés]
[31 de mayo de 2021]

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 penetra cada vez más en nuestras vidas, muchos de los problemas que enfrentamos en el mundo físico surgen también en el ciberespacio. El ciberespacio se explota cada vez más con fines políticos e ideológicos, y el aumento de la polarización a nivel internacional está impidiendo un multilateralismo eficaz. El panorama de las amenazas se ve agravado por las tensiones geopolíticas sobre la Internet mundial y abierta y sobre el control de las tecnologías en toda la cadena de suministro. Los ataques malintencionados dirigidos contra infraestructuras críticas 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 tecnologías de la información y las comunicaciones (TIC), amenazan el ciberespacio global y abierto, así como el estado de derecho, los derechos fundamentales, la libertad y la democracia. 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 aumentan los riesgos de conflicto.

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

La Unión Europea y sus Estados miembros apoyan firmemente la visión antes mencionada de un ciberespacio abierto, libre, 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 entre los Estados. 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 estrategia de ciberseguridad “Un ciberespacio abierto, protegido y seguro”[13], 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. 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[14] 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 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. 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

[13] 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”.

[14] 6122/15 Conclusiones del Consejo sobre la Ciberdiplomacia.

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" [15] 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.

La preocupación por esos problemas 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 [16]. 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 mundial, abierto, estable, pacífico 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.

En diciembre de 2020, la Unión Europea describió en mayor detalle su estrategia para una transformación digital cibersegura en un entorno de amenazas complejas [17]. La estrategia de ciberseguridad de la Unión Europea para la década digital tiene como objetivo promover y proteger un ciberespacio mundial, abierto, libre, 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

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

[16] 10474/17. Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la Unión Europea a las actividades informáticas malintencionadas ("conjunto de instrumentos de ciberdiplomacia").

[17] Véase la comunicación conjunta al Parlamento Europeo y al Consejo, titulada "La Estrategia de Ciberseguridad de la UE para la Década Digital" y 7290/21 (22 de marzo de 2021), "Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital".

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 mundial, abierto, 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 promover un debate multilateral eficaz que impulse la paz y la seguridad en el ciberespacio, es evidente que se necesita hacer avanzar el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio. 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 la Asamblea General, el programa de acción ofrece una plataforma permanente para la cooperación y el intercambio de mejores prácticas dentro de las Naciones Unidas. Ofrece la oportunidad de impulsar programas de fomento de la capacidad 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.

Contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales

Amenazas existentes y nuevas amenazas

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, los recientes acontecimientos en el ciberespacio presentan desafíos en constante evolución.

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.

Mientras continúa la pandemia de enfermedad por coronavirus (COVID-19), la Unión Europea y sus Estados miembros han observado ciberamenazas y actividades cibernéticas maliciosas dirigidas a operadores esenciales de los Estados miembros y sus asociados internacionales, incluso en el sector de la atención de la salud. La Unión Europea y sus Estados miembros están especialmente alarmados 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.

La Unión Europea y sus Estados miembros condenan este comportamiento malintencionado en el ciberespacio y subrayan su continuo apoyo al aumento de la ciberresiliencia mundial. Cualquier intento de obstaculizar la capacidad de las infraestructuras críticas es inaceptable y puede poner en peligro la vida de las personas. El uso malintencionado de las TIC socava los beneficios que Internet y el uso de las TIC aportan a la sociedad en general y muestra la disposición de algunos actores a arriesgar de hecho la seguridad y la estabilidad internacionales. Todos los agentes deben abstenerse de realizar actividades irresponsables y desestabilizadoras en el ciberespacio.

La Unión Europea y sus Estados miembros piden a todos los países que ejerzan la debida diligencia y adopten medidas apropiadas contra quienes realicen esas actividades desde su territorio, de conformidad con el derecho internacional y los informes de los Grupos de Expertos Gubernamentales de las Naciones Unidas aprobados por consenso de 2010, 2013 y 2015. La Unión Europea y sus Estados miembros insisten una vez más en que los Estados no deben permitir a sabiendas que su territorio se utilice para cometer hechos internacionalmente ilícitos utilizando las TIC y deben también responder a las solicitudes apropiadas de otro Estado para poner fin a las actividades cibernéticas malintencionadas que emanen de su territorio.

Además, como se reconoció en informes anteriores del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, 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 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.

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, como se reconoce en los informes del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015, y los principios establecidos en los párrafos 28 a) a f) del informe de 2015 y en el Grupo de Trabajo de Composición Abierta.

El derecho internacional, incluido el derecho internacional humanitario, que incorpora 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, también en el contexto de un conflicto. La Unión Europea subraya su convicción de que el derecho internacional no es cómplice de la conducta, sino que perfila 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 celebran que el Consejo de Derechos Humanos[18] y la Asamblea General también hayan afirmado estos principios.

Por estas razones, la Unión Europea y sus Estados miembros no piden ni ven la necesidad de que se establezcan nuevos instrumentos jurídicos internacionales para las cuestiones cibernéticas en esta etapa, puesto que ya existe un marco jurídico internacional.

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 en relación con la forma en que se aplica el derecho internacional vigente, ya que esto 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 acerca de las posiciones nacionales con relación a la forma en que el derecho internacional se aplica al uso de las TIC por los Estados, ya que esto promueve la transparencia y fomenta el entendimiento mundial de 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 prestar más atención a la concienciación y capacitación sobre la aplicabilidad del derecho internacional vigente como medio de promover la estabilidad y prevenir los conflictos en el ciberespacio.

Normas, reglas y principios para el comportamiento responsable de los Estados

La Unión Europea y sus Estados miembros alientan a todos los Estados a que aprovechen y promuevan la labor que la Asamblea General ha hecho suya en repetidas ocasiones, en particular en su resolución 70/237, y a que sigan apoyándose en el Grupo de Trabajo de Composición Abierta y promoviendo la aplicación de esas normas y medidas de fomento de la confianza convenidas, que desempeñan un papel esencial en la prevención de conflictos.

La Unión Europea y sus Estados miembros se guiarán, en su uso de las TIC, por el derecho internacional vigente, así como por el cumplimiento de las normas, reglas y principios voluntarios de comportamiento responsable de los Estados y su aplicación en el ciberespacio, tal como se explica en los sucesivos informes del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015. Creemos que para avanzar de una forma práctica se debería alentar una mayor cooperación y transparencia con respecto al intercambio de 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.

[18] A/HRC/RES/20/8.

Medidas de fomento de la confianza

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