Naciones Unidas A/74/120

Asamblea General

Distr. general
24 de junio de 2019
Español
Original: español/francés/inglés

Septuagésimo cuarto período de sesiones
Tema 95 de la lista preliminar*

Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/74/50.

19-10580 (S) 230719 010819

I. Introducción

1. En su septuagésimo tercer período de sesiones, la Asamblea General aprobó dos resoluciones en relación con el tema 96 de su programa sobre sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

2. El 5 de diciembre de 2018, la Asamblea General aprobó la resolución 73/27 relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y el 22 de diciembre aprobó la resolución 73/266 relativa a la promoción de un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.

3. En el párrafo 4 de la resolución 73/27, la Asamblea invitó a todos los Estados Miembros, teniendo en cuenta las evaluaciones y recomendaciones que figuraban 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 Internacional1, a seguir comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

a) La evaluación general de los temas relacionados con la seguridad de la información;

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

c) El contenido de los conceptos mencionados en el párrafo 3 (de la resolución);

d) Posibles medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

4. En el párrafo 2 de su resolución 73/266, la Asamblea invitó a todos los Estados Miembros, teniendo en cuenta las evaluaciones y recomendaciones que figuran en los informes del Grupo de Expertos Gubernamentales, a seguir comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

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

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

5. En cumplimiento de esa solicitud, el 6 de febrero de 2019 se envió una nota verbal a todos los Estados Miembros para invitarlos a proporcionar información sobre el tema. Las respuestas recibidas hasta el momento en que se preparó el informe figuran en la sección II. Las respuestas que se reciban después del 15 de mayo de 2019 se publicarán en el sitio web de la Oficina de Asuntos de Desarme (https://www.un.org/disarmament/ict-security) en el idioma original en que se hayan recibido.

II. Respuestas recibidas de los Gobiernos

Argentina

[Original: español]
[15 de mayo de 2019]

Evaluación general de los temas relacionados con la seguridad de la información

Las tecnologías de la información y las comunicaciones (TIC) brindan oportunidades inéditas para el progreso económico, social, cultural, científico y político, y el avance de dichas tecnologías se encuentra inexorablemente ligado a mayores niveles de desarrollo y bienestar. El ciberespacio se ha convertido en un elemento fundamental en la vida de las personas y las organizaciones, y cada vez más servicios esenciales dependen de las redes informáticas.

No obstante, así como ha permitido niveles de interacción y progreso sin precedentes, el ciberespacio también se encuentra sujeto a una multiplicidad de amenazas de diferente naturaleza y actores que ponen en riesgo la seguridad de las personas, las empresas, las instituciones y los Estados, así como la paz y la seguridad internacionales.

El desarrollo económico, la prestación de servicios esenciales, el bienestar de los ciudadanos y el buen funcionamiento de los organismos estatales dependen fuertemente de la ciberseguridad.

En materia de nuevos riesgos, se advierte un crecimiento de los mismos vinculado a la profusión del uso de dispositivos inteligentes de relativamente bajo costo que permiten el acceso a Internet sin un nivel mínimo de seguridad, lo que aumenta la superficie de potenciales ciberataques.

Este crecimiento requiere acompañamiento de políticas de Estado y de estrategias de responsabilidad corporativa que permitan afrontarlo.

Asimismo, suponen un riesgo adicional los proyectos que impulsan algunos Estados para contar con algún tipo de mecanismo que les permita desencriptar información de dispositivos/aplicaciones y/o contar con mecanismos de puerta trasera (*backdoors*).

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información

En 2017 el Gobierno argentino, mediante el Decreto 577/2017, creó el Comité de Ciberseguridad, presidido por la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros, y en el cual participan la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros, el Ministerio de Defensa, el Ministerio de Seguridad, el Ministerio de Relaciones Exteriores y Culto y el Ministerio de Justicia y Derechos Humanos. Entre las funciones del citado Comité se encuentra la de desarrollar la Estrategia Nacional de Ciberseguridad y elaborar el plan de acción necesario para su implementación.

La creación del Comité de Ciberseguridad posibilitó generar instancias de intercambio de información sobre incidentes que permitieron mejorar la coordinación ante incidentes, la cual se mostró efectiva durante la realización del Grupo de los 20 en la Argentina en 2018.

La Argentina cuenta con un Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, creado en virtud de la resolución 580/2011 de la Jefatura de Gabinete de Ministros, que apunta a definir y proteger la infraestructura estratégica y crítica de los sectores público y privado y de las organizaciones

interjurisdiccionales, así como administrar toda la información sobre reportes de incidentes de seguridad y encauzar sus posibles soluciones de forma organizada y unificada, entre otros objetivos.

En este marco, se ha establecido un protocolo para circunstancias de alta exposición a riesgos de seguridad informática, entre organismos públicos, y que contempla la vinculación con el sector privado.

Actualmente se está trabajando en la elaboración de una norma que aprueba la definición de infraestructuras críticas de información, los criterios para determinar su criticidad y su categorización en diversos sectores.

En el marco del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, se creó por Disposición núm. 2/2013 el Equipo de Respuesta ante Incidencias de Seguridad Informáticas Nacional.

En materia de legislación, el delito cibernético fue incorporado al Código Penal en 2008 mediante la Ley 26.388. En 2013 el Congreso de la Nación sancionó la Ley 26.904, que tipifica el delito de captación de niños por Internet con fines sexuales (*grooming*) y agrava las penas de los delitos vinculados a la pornografía infantil en Internet. En 2017, el Congreso aprobó la Ley 27.411 de adhesión al Convenio sobre la Ciberdelincuencia. En enero de 2019 el Congreso sancionó la Ley 27.482 de modificación del Código Procesal Penal Federal, que incorpora herramientas para la obtención de evidencia digital (interceptación de comunicaciones digitales, registro y conservación de datos y de sistemas informáticos).

Actualmente se está trabajando en un proyecto de ley modificatorio del Código Penal que considera la tipificación de varios delitos informáticos y, particularmente, la afectación de infraestructuras críticas.

A fin de mejorar las capacidades en materia de combate al ciberdelito, el Ministerio de Justicia y Derechos Humanos dictó numerosos talleres de capacitación para operadores del sistema penal sobre ciberdelito, tratamiento de evidencia digital y formas modernas de investigación, junto con organismos internacionales, tales como la Organización de los Estados Americanos (OEA) y el Consejo de Europa. Los talleres se llevaron a cabo en las distintas regiones del país y estuvieron dirigidos a jueces, fiscales y miembros de las fuerzas de seguridad a nivel federal y a nivel provincial. Desde 2016 hasta hoy, estos programas de capacitación alcanzaron a casi 500 jueces y fiscales de todo el país.

Por otra parte, uno de los objetivos de la Agenda Digital Argentina, aprobada por el Decreto 996/2018, es el de desarrollar capacidades en ciberseguridad para generar confianza en los entornos digitales. En este sentido, a fin de fortalecer las capacidades para la concientización/sensibilización sobre los riesgos en el uso de las redes sociales e Internet, con foco en la población en general y en los grupos considerados de riesgo, en particular, se han desarrollado programas de formación de formadores en coordinación con el Programa Punto Digital. Se han abordado temáticas como el ciberacoso (*cyberbullying*), el *grooming*, la suplantación de identidad (*phishing*), la ciberseguridad y estrategias de atención/contención de víctimas/prevención y detección de delitos informáticos, con foco en los jóvenes, los adolescentes y los adultos mayores.

En materia de protección de datos personales, la Argentina fue uno de los primeros países de la región en tener un marco regulatorio de protección de datos personales, mediante la sanción de la Ley 25.326. Participa en el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa.

A partir del 1 de junio de 2019, entrarán en vigor en la República Argentina el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional.

Medidas adoptadas para promover la cooperación internacional en el ámbito de la seguridad de la información

La Argentina promueve el desarrollo de acuerdos a niveles bilateral, regional y multilateral que contribuyan a la generación de un ciberespacio pacífico y seguro, y busca tener presencia en todos los organismos internacionales en materia de ciberseguridad y una participación activa en todos los ámbitos académicos y técnicos internacionales en los que se trabaje la temática.

En este sentido, trabaja activamente en las actividades del Comité del Convenio sobre la Ciberdelincuencia y apoya a los Estados que aún no son partes y quieren adherirse a dicho instrumento. Entre las ventajas concretas que dicho tratado brinda a sus miembros, se encuentra la de formar parte de la Red 24/7, que permite disponer de un canal de cooperación y facilita investigaciones penales entre distintos Estados partes.

No obstante, teniendo en cuenta la naturaleza transnacional del fenómeno del ciberdelito y la necesidad de contar con mecanismos que permitan responder de manera global, la Argentina apoya tanto los procesos en el marco del Convenio sobre la Ciberdelincuencia, como aquellas instancias de discusión que buscan avanzar, en el marco de las Naciones Unidas, hacia la negociación de un marco jurídico universal en la materia (proceso de Viena).

La Argentina ha participado en el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2013 y 2014, y busca contribuir en las discusiones en la Asamblea General relativas a la temática.

Consciente de la centralidad que tiene la creación de capacidades, la Argentina es miembro del Foro Global para la Ciberexperiencia y, junto con la OEA, Chile, México, Estonia y España, participa en la Iniciativa de Ciberseguridad en los Estados miembros de la OEA.

En noviembre de 2018, la Argentina se adhirió al Llamamiento de París para la confianza y la seguridad en el ciberespacio.

A nivel regional, la Argentina participa en las reuniones del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio del Comité Interamericano contra el Terrorismo de la OEA, y ha contribuido a las actividades del Observatorio de la Ciberseguridad en América Latina y el Caribe, aportando información para la segunda edición del estudio *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*, realizado por la OEA y el Banco Interamericano de Desarrollo.

Ha sido sede del II Foro Internacional de Género y Ciberseguridad, organizado juntamente con la OEA, los días 29 y 30 de mayo de 2018.

En el ámbito del Mercado Común del Sur (MERCOSUR), la Argentina ha impulsado la creación de la Agenda Digital del MERCOSUR, en la cual se inscriben también la ciberseguridad.

A nivel bilateral, en 2017 firmó un memorando de entendimiento interinstitucional sobre ciberseguridad con España. Ese mismo año se delineó con los Estados Unidos la conformación de un Grupo de Trabajo Intergubernamental Bilateral sobre Política Cibernética con foco en temas de ciberseguridad, y en 2018 la Argentina firmó un Acuerdo para la Cooperación en Ciberdefensa y Ciberseguridad

y Ciberdelito con Chile. La Argentina considera importante mantener canales abiertos de diálogo en materia de ciberseguridad con todos los países y regiones.

Comentarios relativos al contenido de los informes del Grupo de Expertos Gubernamentales, la resolución 73/27 de la Asamblea General y las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial

La Argentina apoya y comparte el contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales.

Es tarea de los Estados velar por un ciberespacio seguro y pacífico, y para ello es fundamental mantener un comportamiento responsable, mediante la aplicación del derecho internacional vigente, así como mediante el desarrollo de nuevas normas voluntarias, la cooperación internacional y medidas de confianza mutua, conforme a las resoluciones de la Asamblea General 69/28, 70/237, 71/28, 73/187 y 73/266, relacionadas con la cuestión.

La cooperación bilateral, regional y multilateral es fundamental para permitir la creación de capacidad de aquellos Estados que precisen fortalecer sus sistemas de prevención, detección, alerta y respuesta a las amenazas en el ciberespacio.

El combate efectivo del ciberdelito es un elemento esencial para el logro de un ciberespacio seguro y pacífico, y por ello se trata de un asunto de máxima prioridad para la cooperación entre los Estados.

Con relación a la resolución 73/27 de la Asamblea General, en particular al conjunto de reglas, normas y principios internacionales de comportamiento responsable de los Estados que se mencionan en el párrafo 1 de la resolución, se comparte la relevancia de los mismos. Cabe señalar, no obstante, que, atento a la naturaleza de las amenazas en el ciberespacio y el dinamismo con el que evolucionan, resulta adecuado solicitar que los Estados realicen el mayor esfuerzo posible para evitar que su territorio sea utilizado por agentes no estatales para cometer actos internacionalmente ilícitos utilizando las TIC. Sin embargo, no es posible pretender que puedan garantizarlo.

Asimismo, atento al alcance global y transnacional de las amenazas en el ciberespacio, debería reforzarse el énfasis que la comunidad internacional otorga a la creación de capacidad para que todos los Estados, y en particular los países en desarrollo, puedan fortalecer sus sistemas de prevención, detección, alerta y respuesta a las amenazas en el ciberespacio.

La Argentina entiende que es necesario continuar trabajando en el marco de los procesos en las Naciones Unidas, tales como el Grupo de Expertos Gubernamentales y 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, creado en virtud de la resolución 73/27 de la Asamblea General. Es fundamental lograr consensos respecto de cómo se aplica el derecho internacional al ciberespacio, para lo que son necesarios el diálogo y la transparencia respecto de la visión de cada Estado. Asimismo, es crucial desarrollar mecanismos e instrumentos que puedan adaptarse rápidamente a los cambios y los nuevos desafíos que el acelerado avance de la tecnología genera de manera continua.

Colombia

[Original: español]
[15 de mayo de 2019]

Mensajes generales

El Gobierno de Colombia coincide con la necesidad de fortalecer la coordinación y la cooperación entre los Estados para estudiar las amenazas y las posibles medidas de cooperación para encararlas, la aplicación del derecho internacional al uso de las tecnologías de la información y las comunicaciones (TIC) por los Estados, y las normas, reglas y principios de comportamiento responsable de los Estados.

Se considera de la mayor relevancia para la estabilidad internacional que los Estados hagan un uso responsable de las TIC, y que se promueva su uso como un instrumento para el desarrollo económico y social.

Colombia está a favor de un Internet libre, abierto y seguro, siendo fundamental que los países cuenten con las herramientas que les permitan tener una cooperación efectiva en la lucha contra la ciberdelincuencia, que fortalezcan sus capacidades nacionales, y se consoliden las medidas de confianza entre los países.

Es fundamental reconocer y enfrentar los desafíos relacionados con la identidad digital: la cooperación con proveedores de servicios de Internet; la evidencia digital, las técnicas para su obtención, almacenamiento, cadena de custodia, certificación y validez; y la protección de datos, la intimidad y el respeto de los derechos y libertades de las personas, entre otros.

Sin embargo, se considera que los debates referidos al delito cibernético deben seguir siendo discutidos desde el punto de vista técnico y político en la Comisión de Prevención del Delito y Justicia Penal a través del grupo intergubernamental de expertos sobre ciberdelincuencia como foro principal, y no generar nuevos grupos alternos que limiten la participación de los países, así como en el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

Colombia tiene interés en participar en los debates internacionales que se adelanten en el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y en el Grupo Intergubernamental de Expertos. Para este último, Colombia presentó un candidato. En caso de que no sea posible su participación en este último escenario, los aportes se canalizarían a través de los espacios de consulta regional que para el efecto disponga la Organización de los Estados Americanos (OEA).

Observaciones respecto a las resoluciones de la Asamblea General 73/266, sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, y 73/27, sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

El Gobierno de Colombia coincide en la necesidad de mejorar la coordinación y la cooperación entre los Estados para promover el uso responsable de las TIC por parte de los Estados, como elemento fundamental para la estabilidad internacional, así como para que las TIC sean un verdadero instrumento para el desarrollo económico y social.

Colombia fue participante activo del Grupo Intergubernamental de Expertos en el período 2014-2015, en el cual se obtuvo el último documento de contexto, y

coincide plenamente con los conceptos, consideraciones, interpretaciones y recomendaciones consignados en el mismo.

La posición del Gobierno de Colombia es que el derecho internacional debería aplicarse a lo “virtual” al igual que rige para el mundo “físico”. Esta línea o visión no solo ha sido considerada por los expertos del Grupo Intergubernamental de Expertos que alcanzaron un consenso en cuanto a sus aspectos básicos de aplicabilidad, sino que también se evidencia en las medidas de fomento de la confianza de la Organización para la Seguridad y la Cooperación en Europa y la Asociación de Naciones de Asia Sudoriental y la declaración de Lucca del Grupo de los Siete sobre el comportamiento responsable por parte de los Estados en el ciberespacio, y tuvo apoyo unánime del grupo de expertos del Manual de Tallin 2.0. En todo caso, la aplicabilidad de los aspectos asociados al derecho internacional aplicable a las ciberoperaciones efectivamente requiere mayor estudio a efecto de superar “zonas grises” o posible divergentes interpretaciones en su aplicación.

Para los países menos desarrollados tecnológicamente, resulta de primordial importancia que se logren los acuerdos que eviten que el ciberespacio se convierta en un escenario de conflicto incremental, por los posibles efectos que tendría el hecho de ser afectados, ya sea como objetivos de ciberoperaciones en su contra o por ser usados como “Estados *proxy*” por la insuficiencia de capacidades para evitarlo.

En países menos desarrollados tecnológicamente, una afectación a determinada infraestructura crítica cibernética puede tener un impacto de grandes proporciones, no solamente por la dependencia de tecnologías de información y la migración a la automatización de procesos industriales con tecnologías conectadas a Internet, sino por la falta de conciencia sobre los riesgos y amenazas, así como de recursos para fortalecer la seguridad digital de las empresas a cargo de estas infraestructuras.

Se considera fundamental fomentar la discusión al más alto nivel de lo que implica la Carta de las Naciones Unidas y su aplicabilidad para el mantenimiento de la paz y la estabilidad para el fomento de un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones.

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

Con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, el Gobierno nacional expidió en 2011 el documento 3701 del Consejo Nacional de Política Económica y Social, “Lineamientos de política para ciberseguridad y ciberdefensa”. Esta política concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética. A continuación, se presentan de manera general los avances en la implementación de dichos lineamientos de política y las actividades de revisión de los mismos durante 2014 y 2015.

El objetivo general del documento 3701 fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacionales en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: a) implementar instancias apropiadas para prevenir, coordinar, atender, controlar y regular los incidentes o emergencias cibernéticos y generar recomendaciones para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y la ciberdefensa nacionales; b) brindar capacitación especializada en seguridad de la información y

ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y c) fortalecer la legislación en materia de ciberseguridad y ciberdefensa y la cooperación internacional, y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Como evolución de esta política, y con una nueva visión derivada de las mejores prácticas internacionales, y en especial atendiendo principios y recomendaciones de organizaciones multilaterales como la Organización del Tratado del Atlántico Norte (OTAN), la Organización de Cooperación y Desarrollo Económicos, la Unión Internacional de Telecomunicaciones y la OEA y gremios globales del sector privado que han analizado cómo abordar la seguridad digital bajo las condiciones actuales del entorno digital, el Gobierno nacional emitió en 2016 el documento 3854 del Consejo Nacional de Política Económica y Social, "Política nacional de seguridad digital", cuya vigencia va hasta diciembre de 2019 y que se fijó como objetivo fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Para desarrollar el objetivo general de la política pública en mención, se plantearon los siguientes objetivos específicos: a) establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos; b) crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital; c) fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos; d) fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos; y e) generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.

Desde el momento de su aprobación por el Consejo Nacional de Política Económica y Social en abril de 2016, se han venido adelantando actividades previstas en el plan de acción y seguimiento que acompaña la política nacional de seguridad digital por parte de las entidades públicas responsables, con el fin de lograr tanto el objetivo general como los objetivos específicos de la política.

En resumen, del conjunto de acciones establecidas, se pueden destacar los siguientes logros:

- Se inició el establecimiento de un marco institucional articulado que involucra a las múltiples partes interesadas para la implementación de la política nacional de seguridad digital, en particular creando la figura del Coordinador Nacional de Seguridad Digital en la Presidencia de la República y asegurando la continuidad de las operaciones del Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- Se inició el proceso para el diseño y la implementación en el Gobierno nacional de un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco conceptual de esta política, los estándares de seguridad internacionales y el marco de gestión de riesgos integral a nivel nacional.
- Se empezaron a crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, en particular adelantando un estudio sobre el impacto de los delitos y crímenes en el entorno digital en el país

y ajustando el marco regulatorio del sector TIC en torno al tema de la seguridad digital.

- Se elaboraron planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica de las instancias que forman parte de la institucionalidad actual en el Gobierno nacional.

- Se han suscrito convenios de cooperación internacional con países aliados y con importantes representantes de la industria, orientados al fortalecimiento de capacidades y el intercambio de información sobre amenazas. En 2017 la OTAN aprobó de forma unánime la firma de un programa de colaboración y cooperación individual con Colombia, siendo nuestro país el primer país de América Latina en adquirir este estatus, integrándose como socio global. En el marco de este instrumento jurídico, uno de los puntos incluidos es la mejora de las competencias en materia cibernética. Para Colombia es fundamental el fortalecimiento de las iniciativas existentes y vigentes en diversos escenarios en el marco de las Naciones Unidas.

Respecto al objetivo de establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos, se identifican progresos como la creación de la figura del Coordinador Nacional de Seguridad Digital (dotado de herramientas técnicas y jurídicas), así como la creación de un Comité de Seguridad Digital como órgano del consejo de gestión y desempeño de la función pública e instancia de máximo nivel interinstitucional e intersectorial en el Gobierno nacional para la orientación superior en temas de seguridad digital. De igual manera, se evidencia el diseño de instrumentos claves como el modelo de gestión de riesgos de seguridad digital de obligatoria adopción e implementación por parte de las entidades de orden nacional del sector ejecutivo, el cual fue incorporado por el Departamento Administrativo de la Función Pública en la *Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas* en agosto de 2018.

Como retos se identifica la necesidad de implementar y fortalecer la gestión de riesgos de seguridad digital en las instancias encargadas de la ciberseguridad y la ciberdefensa de la institucionalidad creada. También la necesidad de fortalecer las capacidades sectoriales mediante un ejercicio más eficiente de promoción y creación de equipos de respuesta a incidentes de ciberseguridad sectoriales, establecer una hoja de ruta eficiente para el efectivo desarrollo del Comité de Seguridad Digital, establecer un protocolo efectivo entre los enlaces sectoriales y territoriales con la coordinación nacional de seguridad digital, así como identificar, valorar y hacer una gestión efectiva de los riesgos por parte de todas las múltiples partes interesadas.

Respecto al segundo objetivo, relacionado con la creación de condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, se identifican algunos avances respecto de la formulación de un borrador de agenda nacional de seguridad digital. Sin embargo, se requiere continuar fortaleciendo la vinculación en las discusiones de todas las múltiples partes interesadas, contar con más aportes académicos (investigaciones) sobre la materia y que se acompañe a las entidades públicas en la adopción del modelo de gestión de riesgos de seguridad digital. Se han adelantado algunas campañas de sensibilización, como el programa “En TIC confío”, y adicionalmente, se elaboró con el apoyo de la OEA el *Estudio sobre el Impacto Económico de los Incidentes, Amenazas y Ataques Cibernéticos en Colombia* para el año 2017 y se está elaborando el mismo estudio para el año 2018.

Como retos se aprecia que es necesario identificar líneas de investigación que deben continuar y fortalecerse en torno a la seguridad digital, identificar un modelo claro y efectivo de coordinación y comunicación que permita establecer un marco legal necesario en materia de seguridad digital que promueva la transformación digital de las múltiples partes interesadas, comunicar eficientemente los resultados de estudios estratégicos en los altos niveles del Gobierno para toma de decisiones y reorientar la estrategia para la creación de contenidos educativos que se incluyan en los currículos académicos desde los diferentes niveles de formación educativa.

Respecto al tercer objetivo, relacionado con el fortalecimiento de la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos, existen progresos frente al diseño de planes de fortalecimiento de capacidades de instancias clave, frente a reportes de estadísticas de cibercrimen y frente al fortalecimiento de capacidades en gestión de riesgos para los responsables de la ciberseguridad en el país.

Como reto se identifica la urgente ejecución de los planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica diseñados para las instancias y entidades responsables de la ciberseguridad, así como la definición de lineamientos de ajuste al marco legal y regulatorio vigente para adecuarlos a las necesidades en materia de: a) análisis, anticipación, prevención, detección, atención e investigación de delitos cibernéticos, cibercrímenes y de fenómenos en el entorno digital y de delitos y crímenes que utilicen el entorno digital como medio; b) persecución y criminalización de nuevos tipos delictivos que incluyan los delitos informáticos como delitos fuente de lavado de activos, y c) actuación de los organismos de seguridad, defensa del Estado e inteligencia en el entorno digital, de acuerdo con los principios fundamentales de la política nacional de seguridad digital.

Respecto al cuarto objetivo, relacionado con el fortalecimiento de la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos, se evidencian progresos en el diseño de planes de fortalecimiento de capacidades de instancias claves, en la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales, en la creación de algunos contenidos de los planes de protección de la infraestructura crítica cibernética, en la creación de algunos equipos de respuesta a incidentes de ciberseguridad sectoriales para fomentar la adecuada gestión de incidentes digitales en las infraestructuras críticas cibernéticas nacionales (tales como las del Gobierno, del sector financiero y del sector eléctrico) y en la participación de algunas partes interesadas en ejercicios de simulación y entrenamiento, a nivel nacional e internacional, para desarrollar habilidades y destrezas para las múltiples partes interesadas responsables de las infraestructuras críticas cibernéticas nacionales y la defensa nacional en el entorno digital.

Como retos frente a este objetivo se evidencia que es necesario reorientar desde el más alto nivel los lineamientos en materia de protección y defensa de las infraestructuras críticas cibernéticas nacionales teniendo en cuenta las nuevas condiciones, y expedir oficialmente un protocolo de gestión y respuesta a incidentes de seguridad digital a este tipo de infraestructuras. De igual manera, es necesario establecer una estrategia en la cual el Gobierno nacional unifique las acciones de sensibilización y formación en materia de seguridad digital en el ámbito de la defensa nacional.

Finalmente, respecto al quinto objetivo, relacionado con la generación de mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional, se aprecian avances en la adhesión a mecanismos para impulsar la cooperación, colaboración y asistencia a nivel internacional, en materia de seguridad digital. Se aprecian progresos tales

como el proceso de adhesión al Convenio sobre la Ciberdelincuencia, y un avance en la preparación de un borrador de agenda estratégica de cooperación, colaboración y asistencia internacional.

En cuanto a los retos, se hace necesario identificar y priorizar los escenarios en los que Colombia debe participar en materia de seguridad digital e identificar un modelo claro y efectivo de coordinación y comunicación entre partes interesadas que permita elaborar e implementar documentos estratégicos para impulsar la cooperación, la colaboración y la asistencia, tanto a nivel nacional como internacional, en asuntos de seguridad digital.

Teniendo en cuenta todo lo anterior, y dado que la política nacional de seguridad digital establecida en el documento 3854 del Consejo Nacional de Política Económica y Social de 2016 tiene un plan de acción que termina en 2019, el Gobierno nacional, con apoyo de la OEA, está en el proceso de elaboración de una nueva política que aborde los retos citados.

Cuba

[Original: español]
[29 de abril de 2019]

Las nuevas tecnologías de la información y las comunicaciones (TIC) deben ser utilizadas de manera pacífica por el bien común de la humanidad y para promover el desarrollo sostenible de todos los países, cualquiera que sea su nivel de desarrollo científico y tecnológico.

Dichos avances científicos y tecnológicos pueden tener aplicaciones civiles y militares y hay que impedir que este progreso afecte la seguridad internacional de los Estados.

El único camino para evitar que el ciberespacio se convierta en un teatro de operaciones militares es la cooperación mancomunada entre todos los Estados.

En este sentido, respaldamos la creación de un Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, en virtud de la resolución 73/27 de la Asamblea General, con miras a que el proceso de negociación de las Naciones Unidas sobre la seguridad en la utilización de las TIC sea más democrático, inclusivo y transparente.

Consideramos necesario establecer un marco regulador internacional jurídicamente vinculante, complementario al derecho internacional existente, aplicable a las TIC.

Todos los Estados deben respetar las normas internacionales existentes en esta esfera. Los accesos a los sistemas de información o de telecomunicaciones de otro Estado deben corresponderse con los acuerdos de cooperación internacional alcanzados, sobre la base del principio del consentimiento del Estado concernido. Las formas y el alcance de los intercambios deben respetar la legislación del Estado a cuyo sistema se accederá.

El uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente acordadas en esta materia y constituye un uso ilegal e irresponsable de estos medios.

Mediante transmisiones radiales y televisivas ilegales, se ha estado agrediendo de modo permanente desde el exterior el espacio radioeléctrico cubano, difundiendo programaciones especialmente diseñadas para incitar al derrocamiento del orden constitucional establecido por el pueblo cubano.

Como promedio, durante 2018 se transmitieron de manera ilegal contra Cuba 1.653 horas semanales a través de 20 frecuencias desde el territorio de los Estados Unidos, en contravención de los propósitos y principios de la Carta de las Naciones Unidas, el derecho internacional y las disposiciones de la Unión Internacional de Telecomunicaciones.

Una vez más, Cuba exhorta a que se ponga fin de inmediato a estas políticas agresivas y lesivas a la soberanía de Cuba, que resultan, además, incompatibles con el desarrollo de vínculos respetuosos y de cooperación entre los Estados.

El bloqueo económico, comercial y financiero impuesto por el Gobierno de los Estados Unidos contra Cuba, por casi 60 años, ha causado severas afectaciones al pueblo cubano, incluido en el uso y disfrute de las TIC.

Las Jefas y los Jefes de Estado y de Gobierno de América Latina y el Caribe, en la Segunda Cumbre de Jefes de Estado y de Gobierno de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), proclamaron a la región de América Latina y el Caribe como zona de paz, entre otros objetivos, para fomentar las relaciones de amistad y de cooperación entre sí y con otras naciones, independientemente de las diferencias existentes entre sus sistemas políticos, económicos y sociales o sus niveles de desarrollo, practicar la tolerancia y convivir en paz como buenos vecinos.

Durante la Quinta Cumbre de Jefes de Estado y de Gobierno de la CELAC, celebrada en Punta Cana (República Dominicana), en enero de 2017, se destacó nuevamente la importancia de las TIC, incluido el Internet, como herramientas para fomentar la paz, el bienestar humano, el desarrollo, el conocimiento, la inclusión social y el crecimiento económico.

Egipto

[Original: inglés]
[9 de mayo de 2019]

Introducción

En los últimos tres decenios, el mundo ha sido testigo de un aumento espectacular del uso de Internet, los teléfonos inteligentes y los modernos aparatos de tecnología de la información y las comunicaciones (TIC), junto con una abrumadora cantidad de usos de las TIC en los ámbitos de los negocios, el comercio, los servicios públicos, la educación, el conocimiento, el entretenimiento, el turismo, la atención de la salud y otras actividades económicas, sociales y culturales. Además de las oportunidades que ofrece el continuo crecimiento del uso de las telecomunicaciones e Internet y la proliferación de las transacciones y los servicios electrónicos, es importante ser consciente de las amenazas y los desafíos que afectan a la infraestructura de las TIC y a las transacciones electrónicas en general y encararlos, pues socavan la confianza en los servicios electrónicos y, en particular, en las transacciones electrónicas.

Por lo tanto, Egipto atribuye gran importancia al importante papel que desempeña el desarrollo y la aplicación de las tecnologías de la información y los medios de telecomunicación más recientes para lograr el progreso económico y social en los planos nacional e internacional. Egipto también apoya activamente la utilización de las TIC para el bien común de la humanidad y para promover el

desarrollo sostenible de todos los países, independientemente de su nivel de desarrollo científico y tecnológico. Además, Egipto considera que las Naciones Unidas deben desempeñar un papel central en la dirección de los esfuerzos internacionales pertinentes y en la promoción del diálogo entre los Estados Miembros para llegar a un entendimiento internacional común sobre la aplicación de las leyes y normas internacionales, las reglas y los principios de un comportamiento responsable de los Estados en la esfera de la información, incluida la aplicación de instrumentos jurídicamente vinculantes.

Los retos y amenazas cibernéticos más importantes

1. Amenaza de penetración y sabotaje de la infraestructura de las TIC

Recientemente han surgido nuevos tipos de ciberataques extremadamente graves, destinados a perturbar servicios críticos y a desplegar programas maliciosos y virus para destruir o perturbar la infraestructura de las TIC y los sistemas críticos de control industrial, especialmente en instalaciones clave, incluidas las entidades de energía nuclear, petróleo, gas natural, electricidad, aviación, diversas formas de transporte, bases de datos nacionales de importancia clave, los servicios gubernamentales, la atención sanitaria y los servicios de ayuda de emergencia. Estos ciberataques despliegan varios canales, incluidos las redes inalámbricas y la memoria móvil, y otros canales comunes como el correo electrónico, los sitios web, los medios sociales y las redes de telecomunicaciones, lo que puede tener un efecto considerable en la utilización de la infraestructura crítica y los servicios y empresas asociados. En la práctica, las instalaciones vitales pueden ser vulnerables a ciberataques avanzados, incluso si no están conectadas directamente a Internet.

2. Amenaza de ciberterrorismo y ciberguerra

Recientemente, se han extendido tipos peligrosos de ciberataques y ciberdelitos, en que se utilizan tecnologías avanzadas, como la computación en la nube, las escuchas telefónicas y los dispositivos de intrusión en la red, el cifrado avanzado y las herramientas de piratería informática automatizada dirigidas a los sistemas informáticos y las bases de datos. Además, se pueden desplegar programas maliciosos avanzados (*malware*) para socavar los sistemas de seguridad de la red y comprometer los sistemas informáticos para crear computadoras zombis, que pueden utilizarse más tarde en una variedad de actividades delictivas e ilegales. Una red automatizada de computadoras zombis puede consistir en decenas, cientos de miles o millones de equipos comprometidos que pueden utilizarse para lanzar ciberataques graves, como los ataques de denegación de servicio distribuidos contra redes y sitios web específicos con fines destructivos, terroristas o de extorsión.

El desarrollo de virus informáticos complejos y sofisticados a menudo requiere niveles avanzados de conocimientos y experiencia no convencional, disponibles solo en países tecnológicamente avanzados, para ser utilizados con fines tácticos, estratégicos y bélicos, así como además de los ataques militares convencionales, o a veces en lugar de ellos, en lo que se conoce como ciberguerra o guerra cibernética. Sin embargo, esas tecnologías maliciosas están siendo transferidas, copiadas o reproducidas por organizaciones terroristas para su utilización en operaciones terroristas y por la delincuencia organizada, así como para amenazar y perturbar las infraestructuras de las TIC con fines de extorsión o espionaje industrial o con ambos fines. Egipto reafirma las posiciones expresadas por los principales expertos en ciberseguridad que esperan una mayor proliferación de ataques cibernéticos feroces y sofisticados en un próximo período.

3. La amenaza del robo de identidad digital y de datos privados

El robo de identidad digital es uno de los delitos más graves que amenazan a los usuarios de Internet y el futuro de los servicios electrónicos. El robo de credenciales y datos personales puede facilitar la suplantación de personas en el ciberespacio y dar lugar a pérdidas monetarias y patrimoniales o enmarañar los nombres de las víctimas en actividades sospechosas o ilegales. El ladrón de identidad suele utilizar información que ya está disponible en Internet, especialmente en los medios sociales abiertos y las redes profesionales; bases de datos nacionales; las redes de servicios públicos, los servicios de seguridad social y atención de la salud; los sitios web de comercio electrónico; los mercados virtuales; las redes de pago electrónico; los cajeros automáticos; y los mercados bursátiles. Además, las herramientas y los sistemas utilizados para realizar transacciones electrónicas pueden verse comprometidos, robados o dañados, lo que supone una grave amenaza para los intereses de los usuarios y el futuro de los servicios electrónicos. Los ataques extensos y generalizados pueden afectar al sector financiero nacional. Los datos de las instituciones públicas y las empresas también pueden ser robados, lo que ocasiona considerables pérdidas materiales y de credibilidad y daño a la reputación, el desgaste y la pérdida de clientes y la reducción del valor de los activos intangibles, lo que puede perjudicar a la economía nacional en su conjunto.

Aspectos fundamentales de la gravedad de las nuevas amenazas cibernéticas

Las nuevas amenazas cibernéticas pueden ser muy graves debido a tres aspectos principales:

1. Suelen desplegar tecnologías sofisticadas y avanzadas; los países altamente desarrollados y las grandes empresas suelen tener el monopolio de estas tecnologías. Muchas de estas tecnologías son ultrasecretas y no están disponibles para la exportación. Además, las versiones exportables de algunas tecnologías pueden contener puertas traseras (*backdoors*) o vulnerabilidades que las convierten en una fuente de amenazas adicionales.

2. Pueden propagarse fácilmente, y la rápida propagación de virus maliciosos y el lanzamiento de ataques distribuidos de denegación de servicio y otros ataques cibernéticos avanzados pueden ocurrir con rapidez y facilidad, debido al uso generalizado de las tecnologías de la información y las comunicaciones y a la facilidad de lanzar esos ataques a distancia y transmitir virus a través de las fronteras desde cualquier lugar y a bajo costo. También es difícil y a veces imposible rastrear a tiempo el origen principal de esas amenazas y riesgos para enfrentar y superar esos problemas.

3. Pueden tener un efecto generalizado; los ataques cibernéticos pueden tener amplias repercusiones directas e indirectas sobre la infraestructura, pues causan daños y pérdidas importantes. Además, pueden ejecutarse a distancia y expandirse repentinamente de una manera imprevisible, afectando potencialmente a entidades fundamentales y a un gran número de ciudadanos (miles o millones).

El camino a seguir para encarar los retos cibernéticos

Los ataques y los delitos cibernéticos pueden trascender las fronteras geográficas de los países y suelen basarse en redes de delincuencia organizada tradicionales y técnicas. El enfrentamiento de esos ataques y delitos deberá incluir, por lo tanto, los mecanismos tradicionales de cooperación internacional para combatir los delitos y hacer frente a las amenazas cibernéticas, así como marcos legislativos y reglamentarios con mecanismos especiales para manejar los avances tecnológicos emergentes. La respuesta eficaz a los ataques cibernéticos y la ciberdelincuencia requiere la cooperación y la coordinación a nivel nacional entre los asociados que proporcionan y operan la infraestructura en sectores críticos y los asociados que

prestan servicios, incluidos los organismos, instituciones y empresas gubernamentales. Además, la cooperación y la coordinación a escalas internacional y regional son sumamente esenciales y deben incluir a organizaciones internacionales claves, reuniones regionales y foros internacionales especializados y de profesionales.

Las contribuciones de Egipto

Egipto es consciente de la importancia de la cooperación internacional para hacer frente a los desafíos en materia de ciberseguridad. Los expertos egipcios han contribuido a varios grupos de expertos gubernamentales pertinentes a los que la Asamblea General ha encomendado la tarea de formular recomendaciones convenidas sobre la ciberseguridad desde la perspectiva de la seguridad internacional. Además, como miembro de la Unión Internacional de Telecomunicaciones (UIT), Egipto formó parte del Grupo de Expertos de Alto Nivel sobre Ciberseguridad de la UIT y participó en actividades de su Programa Mundial de Ciberseguridad. Además, Egipto propuso la creación del Grupo de Trabajo del Consejo de la UIT sobre Protección de la Infancia en Línea y presidió el Grupo de 2010 a 2017. Egipto también participa en ciberejercicios y conferencias y talleres regionales sobre ciberseguridad, algunos de los cuales ha acogido en su territorio, organizados por organizaciones internacionales como la UIT, la Organización de Cooperación Islámica, la Organización para la Seguridad y la Cooperación en Europa, la Organización de Cooperación y Desarrollo Económicos y el Foro de Equipos de Seguridad y Respuesta a Incidentes. Asimismo, Egipto participa en estudios internacionales y regionales sobre ciberseguridad con organizaciones profesionales como la Asociación del Sistema Global de Comunicaciones Móviles. Además, Egipto participa activamente en los esfuerzos regionales en contextos africanos y árabes para promover medidas de transparencia para el fomento de la confianza y la creación de capacidad y la difusión de las mejores prácticas. Egipto también ha entablado consultas y negociaciones bilaterales con varios Estados y organizaciones y asociados internacionales para concertar acuerdos de cooperación bilateral en este ámbito estratégico.

A nivel nacional, y a la luz del artículo 31 de la constitución egipcia, a finales de 2014 se creó un Consejo Supremo para la Protección de la Infraestructura Vital de la Información y la Ciberseguridad (a saber, el Consejo Supremo de Ciberseguridad de Egipto) a nivel del gabinete ministerial. El Consejo está presidido por el Ministro de Comunicaciones y Tecnología de la Información y cuenta con miembros de los sectores vitales, así como de los principales organismos de seguridad. A nivel operativo, el Equipo Nacional de Preparación para Emergencias Informáticas se ha convertido en el brazo técnico del Consejo. El Consejo elaboró la primera estrategia nacional de ciberseguridad de Egipto en 2017. El alcance, la estructura y los objetivos de la estrategia están en consonancia con las necesidades nacionales y se ajustan a los principios, reglas y normas internacionales. Asimismo, la aplicación de la estrategia sigue el mismo espíritu.

Conclusión

Egipto reitera la urgente necesidad de intensificar la creación de capacidad y la asistencia técnica a los países en desarrollo en el ámbito de la seguridad de las TIC, especialmente teniendo en cuenta que, en muchos casos, la seguridad del ciberespacio puede ser tan sólida como su eslabón más débil.

Además, la eficaz labor del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y los informes finales pertinentes transmitidos por el Secretario General a la Asamblea General representan pasos importantes en la dirección correcta. Lo principal es destacar la importancia central de los compromisos de los Estados con los principios de la Carta de las Naciones Unidas y otros principios

del derecho internacional, en particular la igualdad soberana; la solución de controversias internacionales por medios pacíficos; la renuncia a recurrir, en las relaciones internacionales, a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas; el respeto de los derechos humanos y las libertades fundamentales, y la no intervención en los asuntos internos de otros Estados. El objetivo final es lograr un entorno de tecnología de la información y las comunicaciones fiable y seguro, en consonancia con la necesidad de preservar la libre circulación de la información.

Habida cuenta de la gravedad de las nuevas amenazas cibernéticas, Egipto valora y apoya enormemente la recomendación que figura en la resolución 73/27 en el sentido de que se establezca un grupo de trabajo de composición abierta, que actúe por consenso, para seguir desarrollando, con carácter prioritario, las reglas, normas y principios del comportamiento responsable de los Estados con miras a que el proceso de negociación de las Naciones Unidas sobre la seguridad en la utilización de las tecnologías de la información y las comunicaciones sea más democrático, inclusivo y transparente. Además, Egipto espera con interés sumarse a los esfuerzos del grupo de trabajo de composición abierta para encontrar formas de aplicar esas reglas, normas y medidas de fomento de la confianza y apoyarlos.

Egipto también espera con interés participar en las actividades del Grupo de Expertos Gubernamentales establecido en virtud de la resolución 73/266, incluidas las actividades de colaboración con las organizaciones regionales pertinentes mediante una serie de consultas.

Francia

[Original: francés]
[14 de mayo de 2019]

1. Apreciación general de las problemáticas de la ciberseguridad

Como observación preliminar, Francia desea recordar que no utiliza el término “seguridad de la información”, por preferir el de “seguridad de los sistemas de información”, o bien “ciberseguridad”. En efecto, como promotor activo de la libertad de expresión en línea (como lo demuestra el hecho de que fuera copatrocinador de la resolución 38/7 del Consejo de Derechos Humanos en 2018), Francia no considera que la información como tal pueda ser un factor de vulnerabilidad del que sea necesario protegerse, sin perjuicio de las medidas que puedan adoptarse de manera proporcionada, transparente y en condiciones establecidas estrictamente por la ley, de conformidad con el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos.

El término ciberseguridad es, pues, más preciso, en la medida en que se refiere a la capacidad de un sistema de información para resistir a acontecimientos que se originan en el ciberespacio y que pueden poner en peligro la disponibilidad, integridad o confidencialidad de los datos almacenados, tratados o transmitidos y de los servicios conexos que estos sistemas ofrecen o a los que proporcionan acceso. La ciberseguridad utiliza técnicas de seguridad de los sistemas de información y se basa en la lucha contra la ciberdelincuencia y el establecimiento de una ciberdefensa.

Francia considera que el espacio digital debe seguir siendo un espacio de libertad, intercambio y crecimiento que condicione la prosperidad y el progreso de nuestras sociedades. Como ya había subrayado en su estrategia nacional de seguridad

digital[1], en 2015, Francia considera que la tecnología digital, que aporta nuevos usos y nuevos servicios, es un factor de innovación. Provoca un cambio en la mayoría de las profesiones. Transforma los sectores de actividad y las empresas para aportarles mayor flexibilidad y competitividad. Ofrece oportunidades para los miembros de una sociedad mediante la mejora de sus tareas cotidianas gracias a los servicios de comunicación, comercio e información en línea, así como a las oportunidades económicas, gracias a la acentuación de la competencia o a la economía colaborativa.

Este ciberespacio abierto, seguro, estable, accesible y pacífico, que brinda oportunidades económicas, políticas y sociales promovidas por Francia en los últimos tres decenios, se ve amenazado hoy por nuevas prácticas destructivas que se están desarrollando en el ciberespacio. En efecto, las especificidades del espacio digital (anonimato relativo, bajos costos, fácil acceso a herramientas maliciosas, fácil implementación, proliferación de las vulnerabilidades, etc.) permiten a muchos actores desarrollar un arsenal digital con fines de espionaje, tráfico ilícito, desestabilización y sabotaje. Si bien algunas amenazas de bajo nivel no guardan relación con la seguridad nacional, sino con una forma de delincuencia, la utilización de armas cibernéticas dirigidas contra sistemas informáticos estatales, infraestructuras de importancia crítica o grandes empresas puede tener graves consecuencias.

Las cuestiones de ciberseguridad se han convertido en parte integrante de las estrategias de poder y las relaciones de fuerza que rigen las relaciones internacionales; se trata de una prioridad y de una cuestión política importante. Como se destaca en la Revisión Estratégica de la Defensa y la Seguridad Nacional de 2017[2], “la digitalización masiva de nuestras sociedades durante la última década y la interconexión global de los sistemas de información y de comunicación están creando nuevas amenazas y oportunidades. Están poniendo al alcance de todo el mundo poderosas herramientas de expresión, influencia, propaganda e inteligencia, enormes volúmenes de datos, pero también peligrosos vectores de ataque. Alientan el surgimiento de nuevos actores privados, que se imponen en la escena internacional como un desafío a la soberanía de los Estados, pero también como socios a veces esenciales. Transforman efectivamente las relaciones de poder entre los actores estatales, no estatales y el sector privado”.

Todos tenemos una parte de responsabilidad en la preservación, el desarrollo y la promoción de un espacio cibernético abierto, seguro, estable, accesible y pacífico. Frente a las amenazas comunes que afectan a la estabilidad y la seguridad internacionales, Francia aplica desde hace varios años una política y una diplomacia activas con miras a reforzar la seguridad, la confianza y la estabilidad en el ciberespacio.

2. Esfuerzos emprendidos para reforzar la ciberseguridad nacional y promover la cooperación internacional en este ámbito

a) Refuerzo del dispositivo de ciberseguridad francés

En las orientaciones estratégicas adoptadas en los últimos años al más alto nivel del Estado francés se sigue considerando la ciberseguridad como una de las prioridades de la acción gubernamental.

Francia sigue fomentando la potencia y la madurez de su dispositivo nacional. En consonancia con las medidas adoptadas en los últimos diez años (creación y puesta

[1] Se puede consultar en: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

[2] Se puede consultar en: www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.

en marcha del Organismo Nacional de la Seguridad de los Sistemas de Información (*Agence nationale de la sécurité des systèmes d'information*) desde 2009, la elaboración de la primera estrategia francesa de defensa y seguridad de los sistemas de información en febrero de 2011, el fortalecimiento de los instrumentos jurídicos y el aumento sustancial de los recursos asignados a la ciberseguridad por las últimas leyes de programación militar, la publicación en febrero de 2014 del "Pacto de Ciberdefensa" por el Ministerio de Defensa y el desarrollo de un "centro de excelencia cibernética" destinado a estimular el desarrollo de la formación, la investigación académica y la base industrial y tecnológica en materia de ciberseguridad), también aplica una política de transparencia en su estrategia tanto nacional como internacional.

De hecho, desde 2015 Francia adoptó una estrategia nacional de seguridad digital para apoyar la transición digital de la sociedad francesa. En términos de seguridad, destaca la necesidad de una respuesta enérgica contra los actos cibermaliciosos y se propone hacer de la seguridad digital una ventaja competitiva para las empresas francesas.

En diciembre de 2017, la estrategia digital internacional de Francia[3] vino a completar ese documento precisando los principios y objetivos perseguidos por Francia en el ámbito de la tecnología digital a nivel internacional. Estructurada en torno a tres ejes principales (gobernanza, economía y seguridad), esta estrategia tiene por objeto:

- Promover un mundo digital abierto, diversificado y que inspire confianza a escala mundial;
- Afirmar un modelo europeo de equilibrio entre el crecimiento económico, los derechos y libertades fundamentales y la seguridad;
- Reforzar la influencia, el atractivo, la seguridad y las posiciones comerciales de Francia y de los actores franceses en el mundo digital.

En la revista estratégica de ciberdefensa[4] presentada en febrero de 2018 se define una doctrina de gestión de la crisis cibernética y se aclaran los objetivos estratégicos nacionales en materia de ciberdefensa. Confirmando la pertinencia del modelo francés y la responsabilidad primordial del Estado en materia de seguridad cibernética, la doctrina se articula en torno a los siete grandes principios siguientes:

- La mejora de la protección de los sistemas de información de nuestro país;
- La disuasión de los ataques mediante un conjunto de medidas de carácter defensivo, el fortalecimiento de la resiliencia y de la capacidad de reacción y respuesta;
- La afirmación y el ejercicio de una soberanía digital francesa;
- Una respuesta penal más eficaz ante la ciberdelincuencia;
- La promoción de una cultura compartida de seguridad informática;
- La participación en el desarrollo de una Europa digital segura y que inspire confianza;
- Una acción internacional para promover una gobernanza colectiva y controlada del ciberespacio.

[3] Se puede consultar en: www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

[4] Se puede consultar en: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

En la Ley de Programación Militar de 2019-2025[5] se prevé, de conformidad con las leyes anteriores, aumentar considerablemente los recursos asignados a la ciberdefensa, en particular en el ámbito del personal, con un objetivo de contratación de 1.500 personas más para que se alcance la cifra de 4.000 funcionarios asignados a estas cuestiones en el Ministerio de Defensa para 2025.

Los actores siguientes contribuyen a la eficacia del dispositivo técnico y operativo francés:

- El Organismo Nacional de Seguridad de los Sistemas de Información está encargado de la prevención (incluso en materia normativa) de los incidentes informáticos dirigidos contra el Estado y los operadores de importancia vital, y de la reacción ante esos incidentes. Actualmente emplea a 600 personas y sigue creciendo. La Agencia se ha impuesto como referencia para la definición de las normas de ciberseguridad pertinentes.
- El Ministerio de Defensa tiene la doble misión de asegurar la protección de las redes que garantizan su acción y de integrar las operaciones en el ciberespacio que están en el centro de la acción militar. Con el fin de consolidar la acción del Ministerio en este ámbito, en septiembre de 2017 se nombró a un oficial general que está al mando de la ciberdefensa, bajo las órdenes del Jefe de Estado Mayor de las fuerzas armadas. A este respecto, el Ministerio de Defensa publicó, a principios de 2019, una política de guerra informática defensiva y, al mismo tiempo, el Jefe del Estado Mayor de las fuerzas armadas hizo una presentación pública de la doctrina de la guerra informática ofensiva de las operaciones militares.
- El Ministerio del Interior y el Ministerio de Justicia tienen la misión de combatir todas las formas de ciberdelincuencia, centrando la atención en las instituciones e intereses nacionales, los agentes económicos y las colectividades públicas, así como en los particulares.

b) Promoción de la cooperación internacional para la estabilidad y la seguridad del ciberespacio

El refuerzo de la estabilidad estratégica y de la seguridad internacional en el ciberespacio es uno de los objetivos prioritarios de Francia. Como se indica en la revista estratégica de ciberdefensa, “la cooperación de la comunidad internacional en el ciberespacio es un medio eficaz para reforzar su estabilidad mediante un conocimiento mutuo, e incluso una confianza, fortalecida entre los actores y mediante el establecimiento de mecanismos de gestión común de las crisis, de comunicación y de distensión”. La acción de Francia en favor de la cooperación internacional en materia de ciberseguridad se desarrolla en un marco europeo e internacional.

Prevenir las crisis por el refuerzo de las actividades de cooperación y el desarrollo de las capacidades

Francia considera que el principal objetivo de su actuación en el espacio digital es la prevención de las crisis. Así, como se destaca en la Revisión Estratégica de la Defensa Cibernética, “el fortalecimiento de la protección, la resiliencia y la cooperación del conjunto de los actores del ciberespacio es una contribución directa al fortalecimiento de nuestra seguridad nacional”. Para lograr este objetivo, es preciso fortalecer la cooperación técnica, operacional y estructural con los asociados estatales y con las organizaciones internacionales a fin de desarrollar las capacidades respectivas de esos diversos actores y la resiliencia mundial del ciberespacio.

[5] Se puede consultar en: www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte.

En efecto, debido a la gran interconexión de las redes y las sociedades, Francia considera que la ciberseguridad para todos solo estará garantizada cuando cada Estado haya adquirido la capacidad suficiente para garantizar la seguridad de sus propios sistemas de información. Por lo tanto, está trabajando para fortalecer las capacidades de ciberseguridad de sus socios, en el marco de iniciativas bilaterales o multilaterales. Además, esta inversión en cooperación es beneficiosa para todas las partes, pues nos permite mantenernos a la vanguardia del progreso confrontándonos a nuestros pares y aprendiendo de ellos, enriquecer mutuamente los conocimientos y la experiencia y desarrollar la confianza entre los actores interesados.

En el plano técnico, el Organismo Nacional de Seguridad de los Sistemas de Información se propone establecer asociaciones con sus homólogos de numerosos países con el fin de favorecer el intercambio de datos esenciales, como las informaciones relativas a las vulnerabilidades o las fallas de los productos y servicios. Por otra parte, el Centro Gubernamental de Vigilancia, Alerta y Respuesta a Ataques Informáticos del Organismo participa activamente en varias redes multilaterales (Foro de Equipos de Seguridad y Respuesta a Incidentes, equipo de tareas europeo de centros de respuesta a incidentes de seguridad informática, grupo de centros gubernamentales europeos de respuesta a incidentes de seguridad informática, red de centros de respuesta a incidentes de seguridad informática de la Unión Europea), gracias a los cuales mantiene contactos con centros de respuesta a emergencias informáticas de todo el mundo.

En cuanto a la cooperación operativa y estructural, Francia aplica una política voluntarista. En los últimos años, Francia ha enviado expertos técnicos internacionales en ciberseguridad a las fuerzas de seguridad interna de los países socios. Francia también sigue colaborando con el Senegal para poner en marcha las actividades de la Escuela Nacional de Ciberseguridad de Dakar con un enfoque regional, inaugurada a finales de 2018. Este proyecto tiene por objeto proporcionar actividades de formación de corta duración y adaptables a profesionales de la ciberseguridad y a altos funcionarios procedentes prioritariamente de África Occidental.

A nivel de la Unión Europea, a fin de fortalecer la resiliencia cibernética del espacio europeo, Francia contribuye al desarrollo de un marco voluntario de cooperación para la prevención y la resolución de incidentes. Ese marco se basa en particular en el desarrollo de normas operativas comunes y de procedimientos de cooperación entre socios, que son sometidos a prueba en el marco de ejercicios paneuropeos. Francia también ha participado en la elaboración de un “caja de herramientas cibernéticas” que ofrece un marco europeo de respuesta diplomática conjunta ante un ataque informático y se basa en la utilización de medidas de prevención, cooperación y estabilización.

Francia también ha invertido en la adopción de una normativa europea que tenga en cuenta las exigencias de competitividad y el potencial de la tecnología digital, protegiendo al mismo tiempo a los ciudadanos, las empresas y los Estados Miembros (derecho a la intimidad y a la protección de los datos personales, protección de las infraestructuras vitales, lucha contra los contenidos terroristas en línea). Así lo demuestra la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, y de 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, así como la próxima entrada en vigor del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de

ciberseguridad de las tecnologías de la información y las comunicaciones, por el que se deroga el Reglamento (UE) 526/2013 (Reglamento relativo a la ciberseguridad). Francia también apoya activamente la adopción de un reglamento europeo para impedir la difusión de contenidos terroristas en línea e imponer obligaciones uniformes a los operadores de Internet.

Por último, Francia se esfuerza por garantizar que la política industrial de la Unión Europea apoye las capacidades avanzadas de investigación y desarrollo a fin de promover el despliegue de tecnologías y servicios de seguridad digital fiables y evaluados.

En el seno de la Organización del Tratado del Atlántico Norte (OTAN), los aliados adoptaron, a iniciativa de Francia, un compromiso en favor de la ciberdefensa en la Cumbre de Varsovia, celebrada en junio de 2016. Este compromiso garantiza que cada uno de los Estados miembros de la Alianza Atlántica dedique una parte adecuada de sus recursos al fortalecimiento de sus capacidades en materia de ciberdefensa, elevando así el nivel general de seguridad para todos. En mayo de 2018, Francia acogió la primera conferencia dedicada a ese compromiso. Los aliados también han reconocido el ciberespacio como un área de operaciones, comprometiendo a la OTAN a defenderse de la misma manera que lo hace en los ámbitos terrestre, aéreo y marítimo.

Prevenir las crisis mediante la elaboración de normas que regulen el comportamiento de los actores en el ciberespacio

Francia considera que la aparición de un marco de ciberseguridad colectiva solo puede basarse en los equilibrios definidos por el derecho internacional. Además, como se destaca en su estrategia digital internacional, Francia concede importancia a la continuación de un “diálogo de cooperación con todos los actores públicos y privados pertinentes, así como con todos los socios internacionales que estén dispuestos a hacerlo, tanto a nivel bilateral como multilateral”.

Francia ha participado activamente en las negociaciones celebradas en las Naciones Unidas en el marco de las cinco últimas reuniones del Grupo de Expertos Gubernamentales encargado de examinar la evolución de la tecnología de la información y las telecomunicaciones en el contexto de la seguridad internacional. Seguirá participando en la reanudación de los debates, tanto en el Grupo de Expertos Gubernamentales como en el Grupo de Trabajo de composición abierta, para promover su visión de un espacio digital de libertad, intercambio y crecimiento que condicione la prosperidad y el progreso de nuestras sociedades. También participa en otros foros internacionales en que se abordan estas cuestiones de seguridad en el espacio digital.

Francia ratificó en 2006 el Convenio sobre la Ciberdelincuencia, que ofrece una base jurídica para establecer las diferentes infracciones en materia de lucha contra la ciberdelincuencia y prevé los medios flexibles y modernos de cooperación internacional en este ámbito (por ejemplo, la puesta en marcha de una red disponible 24 horas al día para acelerar los procedimientos de asistencia entre los Estados partes). Francia aboga actualmente por la universalización del Convenio, que hoy cuenta con 63 Estados Partes que representan a todos los continentes. Participa activamente en la negociación de su segundo protocolo adicional, cuyo objetivo es reforzar la cooperación internacional en este ámbito mediante el desarrollo de la cooperación policial y la asistencia mutua en materia penal, especialmente en cuanto al acceso a las pruebas electrónicas. Francia también apoya los trabajos del Grupo de Expertos encargado de realizar un estudio a fondo sobre la ciberdelincuencia, que confirmen el papel central de la Oficina de las Naciones Unidas contra la Droga y el Delito en esta esfera.

Presentado por el Presidente de la República en el Foro para la Gobernanza de Internet, celebrado en la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura el 12 de noviembre de 2018, el Llamamiento de París en pro de la Confianza y la Seguridad en el Ciberespacio[6] refleja el papel activo desempeñado por Francia en la promoción de un ciberespacio seguro, estable y abierto. Con ese texto, apoyado hasta la fecha por 66 países y cerca de 500 entidades no estatales, se pretende promover ciertos principios fundamentales de la regulación del espacio digital, como la aplicación del derecho internacional y los derechos humanos en el ciberespacio, el comportamiento responsable de los Estados, el monopolio estatal sobre la violencia legítima y el reconocimiento de las responsabilidades específicas de los actores privados.

Francia también ha participado en la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Trabajó para organizar una primera reunión del Foro Mundial de la OCDE sobre Seguridad Digital para la Prosperidad, en diciembre de 2018, sobre el tema de la responsabilidad de los actores privados en la seguridad digital.

En el marco del Grupo de los Siete (G7), el grupo Ise-Shima, creado en 2016 y dedicado a las cuestiones cibernéticas, permitió que se aprobara en 2017 una declaración ambiciosa, conocida como la declaración de Lucca, relativa a las normas del comportamiento responsable de los Estados en el ciberespacio. En marzo de 2019, en el marco de su presidencia, Francia propuso el establecimiento de un mecanismo de seguimiento de la aplicación de las normas y recomendaciones acordadas al nivel de las Naciones Unidas, de lo que se dejó constancia en la Declaración de Dinard sobre la iniciativa para las normas en el ciberespacio[7].

En el seno del Grupo de los Veinte, Francia está trabajando para garantizar que se aborden las cuestiones fundamentales de la competencia en la economía digital, los nuevos modos de regulación y gobernanza y de la seguridad digital, de conformidad con el Llamamiento de París.

Francia, que participa activamente en el grupo de trabajo oficioso de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre ciberseguridad, sigue promoviendo la aplicación de las 16 medidas de fomento de la confianza elaboradas por la OSCE en relación con los retos cibernéticos. Francia dirige, en particular, la aplicación de una medida de fomento de la confianza en relación con la seguridad de las infraestructuras vitales.

Con el fin de reforzar la lucha contra la proliferación de técnicas y herramientas maliciosas, Francia ha apoyado la inscripción de los programas informáticos de intrusión en la lista de artículos de doble uso del Acuerdo de Wassenaar sobre el control de las exportaciones de armas clásicas y de bienes y tecnologías de doble uso. Francia considera que se debe proseguir el esfuerzo de reglamentación en ese sentido, inscribiendo algunas herramientas cibernéticas, en dependencia de la gravedad de sus efectos, en la lista de los materiales de guerra.

Francia considera que muchas cuestiones relacionadas con la ciberseguridad merecen ser abordadas mediante un enfoque multilateral, a fin de tener en cuenta las funciones y responsabilidades específicas de los agentes no estatales. En el marco de esta lógica, Francia apoya las actividades de la Comisión Global sobre la Estabilidad del Ciberespacio. Esta comisión se encarga de elaborar propuestas de normas y

[6] Se puede consultar en: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.

[7] Se puede consultar en: www.diplomatie.gouv.fr/IMG/pdf/g7_-_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf.

políticas destinadas a reforzar la seguridad y la estabilidad internacionales y a orientar el comportamiento responsable de los Estados en el ciberespacio.

3. Conceptos internacionales pertinentes para reforzar la ciberseguridad mundial

a) Conceptos que permiten preservar la paz y la seguridad internacional

A fin de garantizar un espacio cibernético abierto, seguro, estable, accesible y pacífico, Francia reafirma su adhesión a la aplicabilidad del derecho internacional, incluida la Carta de las Naciones Unidas en su integridad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, al uso de las tecnologías de la información y las comunicaciones por los Estados.

Derecho internacional público

Como concluyó el Grupo de Expertos Gubernamentales de las Naciones Unidas encargado de examinar el desarrollo de la informática y las telecomunicaciones en el contexto de la seguridad internacional en su informe publicado en 2013, los principios y normas del derecho internacional se aplican a la conducta de los Estados en el ciberespacio. Si bien el ciberespacio presenta especificidades propias (anonimato, papel de los agentes privados), el derecho internacional ofrece todos los medios necesarios para encuadrar de manera responsable el comportamiento de los Estados en ese entorno. A este respecto, la falta de atribución no puede constituir un obstáculo definitivo para la aplicación del derecho internacional vigente.

El principio de soberanía se aplica al ciberespacio. A este respecto, Francia reafirma que ejerce su soberanía sobre los sistemas de información, las personas y las actividades cibernéticas en su territorio, dentro de los límites de las obligaciones que le impone el derecho internacional. La penetración no autorizada en sistemas franceses o la producción de efectos en el territorio francés como consecuencia de la utilización de medios cibernéticos por una entidad estatal, o por agentes no estatales que actúan siguiendo instrucciones o bajo el control de un Estado, puede constituir una violación de soberanía.

El alcance de las medidas que los Estados pueden adoptar para responder a un ataque informático del que serían víctimas depende de la gravedad del ataque. Cuanto más grave sea el ciberataque, mayor será el alcance de las medidas. Una operación cibernética puede considerarse un recurso a la fuerza prohibido en virtud del apartado 4 del Artículo 2 de la Carta de las Naciones Unidas. El cruce del umbral del uso de la fuerza no es una función de los medios cibernéticos utilizados, sino de los efectos de la ciberoperación. Si estos últimos son similares a los que resultan de las armas clásicas, la ciberoperación puede constituir un recurso a la fuerza. Francia considera que un ataque informático importante, perpetrado por un Estado o por agentes no estatales que actúan bajo el control o por instrucción de un Estado, que alcance, por su escala o sus efectos, un umbral de gravedad suficiente (por ejemplo, pérdida sustancial de vidas humanas, daños físicos considerables o deficiencia de infraestructuras vitales con consecuencias significativas) y atribuible a un Estado, podría constituir un “ataque armado” en el sentido del Artículo 51 de la Carta, y justificar así la invocación de la legítima defensa. Esta legítima defensa puede llevarse a cabo por medios convencionales o cibernéticos, siempre que se respeten los principios de necesidad y proporcionalidad. La caracterización de un ataque informático como un ataque armado, en el sentido del Artículo 51 de la Carta, depende de una decisión política adoptada caso por caso y a la luz de los criterios establecidos en el derecho internacional.

Francia considera que la creación de un nuevo instrumento internacional jurídicamente vinculante específico para las cuestiones de ciberseguridad no es necesaria en esta etapa. En el ciberespacio, como en los demás ámbitos, el derecho internacional vigente se aplica y debe ser respetado.

Derecho internacional humanitario

Francia apoya la aplicabilidad del derecho internacional humanitario a las operaciones cibernéticas realizadas en el contexto de los conflictos armados y en relación con ellos.

En la actualidad, las operaciones ofensivas de guerra informática son concomitantes con las operaciones militares convencionales. La hipótesis de un conflicto armado que consista exclusivamente en actividades digitales no puede descartarse en principio, sino que depende de la capacidad de las operaciones cibernéticas para alcanzar el umbral de violencia necesario para que se puedan calificar de conflicto armado internacional o no internacional.

A pesar de su carácter desmaterializado, estas operaciones siguen estando sujetas al ámbito de aplicación geográfica del derecho internacional humanitario, es decir, sus efectos se limitan al territorio de los Estados partes en un conflicto armado internacional o al territorio en el que tienen lugar las hostilidades en el contexto de un conflicto armado no internacional.

Las operaciones ofensivas de guerra informática llevadas a cabo por las fuerzas armadas francesas están sujetas al respeto de los principios del derecho internacional humanitario, incluidos los siguientes:

- **El principio de distinción entre bienes de carácter civil y objetivos militares**. En este sentido, se prohíben los ataques cibernéticos que no estén dirigidos contra un objetivo militar específico o que se lleven a cabo con armas cibernéticas que no puedan ser dirigidas contra un objetivo militar específico. A este respecto, algunos datos de contenido, aunque sean de naturaleza intangible, pueden constituir bienes de carácter civil protegidos por el derecho internacional humanitario.

- **El principio de humanidad**. Las operaciones tampoco deben dirigirse contra la población civil como tal o contra civiles, a menos que participen directamente en las hostilidades y durante el tiempo en que lo hagan. En el contexto de un conflicto armado, todo combatiente cibernético de las fuerzas armadas, todo miembro de un grupo armado organizado que cometa ciberataques contra una parte adversa o todo civil que participe directamente en hostilidades por medios cibernéticos puede ser atacado por medios convencionales o cibernéticos.

- **El principio de proporcionalidad.** Las operaciones deben llevarse a cabo con cuidado constante para proteger a las personas y los bienes civiles de los efectos de las hostilidades. Los daños colaterales no deberían exceder la ventaja militar directa y concreta esperada. El respeto del principio de proporcionalidad en el ciberespacio exige que se tengan en cuenta todos los efectos previsibles del arma, ya sean directos (daños al sistema atacado, interrupción del servicio u otros) o indirectos (efectos en la infraestructura controlada por el sistema atacado, pero también en las personas afectadas por el mal funcionamiento o la destrucción de los sistemas, o por la alteración y la corrupción de los datos de los contenidos), a condición de que tengan un vínculo causal suficiente con el ataque. Este principio también prohíbe el uso de armas cibernéticas que no puedan ser controladas (especialmente en el tiempo y el espacio), es decir, que puedan causar daños irreversibles a la infraestructura civil, los sistemas o los datos de contenido civil.

Estos elementos se recuerdan especialmente en los elementos públicos de la doctrina militar francesa de la guerra informática de carácter ofensivo presentados a principios de 2019.

Derechos humanos

Francia sostiene que los derechos de que disfrutan las personas fuera de línea (no conectadas) también deben protegerse en línea y que el derecho internacional de los derechos humanos se aplica al ciberespacio. Estos valores se ven socavados por la difusión en línea de contenidos ilegales (terroristas, antisemitas o que fomentan el odio). Francia considera que es particularmente necesario implicar a los actores privados del mundo digital en la lucha contra los contenidos ilícitos y aclarar su papel y sus responsabilidades en el plano internacional para luchar contra esos contenidos ilícitos y garantizar la protección de los derechos humanos y las libertades fundamentales en línea.

Principio del deber de diligencia

Francia considera esencial lograr una comprensión común, en el plano internacional, de las obligaciones de un Estado cuya infraestructura se utilizara con fines maliciosos contra los intereses de otro Estado. El objetivo es clarificar la aplicación, en el ámbito de la cibernética, del principio de la debida diligencia que preconiza que todo Estado tiene la obligación de "no permitir que su territorio se utilice con fines de actos contrarios a los derechos de otros Estados"[8]. Como tales, los Estados no deben permitir a sabiendas que su territorio se utilice para cometer actos internacionalmente ilícitos por medios cibernéticos y no deben utilizar intermediarios no estatales (*proxys*) para cometer violaciones del derecho internacional. Una mejor comprensión de la aplicación de este principio a las cuestiones cibernéticas permitiría reforzar la cooperación entre los Estados con el fin de proteger determinadas infraestructuras vitales, así como detener los ataques cibernéticos de gran envergadura que transitan por un tercer Estado.

b) Concepto que permite reforzar la cooperación y la confianza entre los Estados

Normas de comportamiento

Las diversas rondas de negociaciones celebradas en el marco del Grupo de Expertos Gubernamentales sobre Ciberseguridad han permitido realizar progresos considerables en la reglamentación internacional del ciberespacio. En el informe de 2015, se describen en particular 11 normas de comportamiento responsable de los Estados en el ciberespacio. Francia considera que cada Estado está obligado a respetar esas normas y a elaborar mecanismos que permitan su aplicación. También podrían elaborarse en el futuro otras normas aplicables al comportamiento de los Estados u otros actores en el ciberespacio.

Medidas de fomento de la confianza

Es preciso seguir profundizando los trabajos en diversos foros y organizaciones regionales con miras a elaborar medidas de fomento de la confianza específicas para las cuestiones de ciberseguridad. Francia seguirá alentando a sus socios para que adopten procedimientos interministeriales que puedan utilizarse para garantizar una buena comunicación entre los Estados en tiempos de crisis. El desarrollo de tales procedimientos y mecanismos, basados en la transparencia y la comunicación, resulta indispensable para la prevención de conflictos en el ciberespacio.

[8] *Affaire du Détroit de Corfou*, Arrêt du 9 avril 1949 : C.I.J., Recueil 1949, pág. 4 (en francés).

Desarrollo de la capacidad

Francia apoya el objetivo de fortalecer la capacidad internacional en materia de ciberseguridad. Estos esfuerzos contribuyen muy directamente al fortalecimiento de la seguridad de todos y a la estabilidad del ciberespacio. Francia se propone participar plenamente en esos esfuerzos mediante actividades de fomento de la capacidad en los planos bilateral, regional o multilateral.

c) Papel y responsabilidad de los actores no estatales

Enfoque multipartito

En el Llamamiento de París, Francia subrayó la necesidad de un enfoque reforzado de actores múltiples. Francia considera, en efecto, que la sociedad civil, el mundo académico, el sector privado y la comunidad técnica disponen de competencias y recursos útiles para definir determinados aspectos de las políticas pertinentes en materia de ciberseguridad.

Responsabilidad en materia de seguridad por parte de los actores privados en el diseño y mantenimiento de los productos digitales

El auge de la tecnología digital como nuevo instrumento y espacio de confrontación otorga al sector privado, en particular a un determinado número de actores sistémicos, un papel fundamental y una responsabilidad inédita en la preservación de la paz y la seguridad internacionales. En el Llamamiento de París, Francia reconoce así "la responsabilidad de los principales actores del sector privado de desarrollar la confianza, la seguridad y la estabilidad en el ciberespacio" y alienta "las iniciativas orientadas a aumentar la seguridad de los procesos, productos y servicios digitales". Francia considera pertinente establecer en el plano internacional un principio de responsabilidad en materia de seguridad de la parte de los actores privados sistémicos en la concepción, la integración, el despliegue y el mantenimiento de sus productos, procesos y servicios numéricos, a todo lo largo de su ciclo vital y de un extremo al otro de la cadena de suministro.

Responsabilidad de las plataformas digitales en materia de lucha contra el terrorismo

Francia también está trabajando para garantizar que los operadores digitales privados asuman una responsabilidad en la lucha contra el uso indebido de sus servicios con fines terroristas. Está planteando este tema en particular en el seno del G7 y de la Unión Europea, donde apoya activamente la aprobación de un proyecto de reglamento europeo que proporcione un marco para la acción de los operadores de Internet en la lucha contra los contenidos terroristas en línea. En este texto se exige la retirada de los contenidos terroristas en el plazo de una hora a petición de un Estado miembro, la adopción de medidas estrictas para las plataformas expuestas a contenidos terroristas, la obligación de designar un punto de contacto disponible las 24 horas del día para tratar las alertas y las solicitudes de retirada, y la imposición de sanciones en caso de falta de cooperación sistemática.

Prevención de las actividades ofensivas por parte de actores privados

Francia considera que los Estados deben mantener el monopolio de la violencia física legítima, tanto en el ciberespacio como en otros ámbitos. En este sentido, apoya la prohibición de que los actores no estatales, incluido el sector privado, realicen actividades ofensivas en el ciberespacio para sí mismos o en nombre de otros actores no estatales. Estas prácticas, basadas en el principio de la legítima defensa privada ("hacking back"), son potencialmente desestabilizadoras debido a sus consecuencias adversas para un tercero y podrían alimentar una posible escalada entre Estados. A

este respecto, Francia considera necesario que se logre aclarar el margen de maniobra de que disponen los actores privados para responder a los incidentes.

4. Medidas que podrían ser adoptadas por la comunidad internacional para reforzar la seguridad cibernética en todo el mundo

Frente a las nuevas amenazas de la revolución digital, Francia considera que la cooperación y el derecho son necesarios para que el ciberespacio no se convierta en una zona de conflicto permanente. Al igual que en otros ámbitos, los Estados deberán respetar el derecho internacional en el espacio digital. Además, en los últimos años ha surgido un corpus normativo que enmarca el comportamiento responsable de los Estados en el ciberespacio, que aún se necesita consolidar. Francia considera que podrían adoptarse las siguientes medidas para reforzar la ciberseguridad a nivel internacional:

- **Profundizar el trabajo realizado en las reuniones precedentes del Grupo de Expertos Gubernamentales**. Sin cuestionar las normas y recomendaciones que han sido objeto de consenso en los ciclos de negociación previos, tal vez sea útil precisar la forma en que estas normas y recomendaciones pueden ponerse en práctica y favorecer una mejor comprensión, en el plano internacional, de las buenas prácticas en la materia.
- **Apoyarse en el Llamamiento de París en pro de la confianza y la seguridad en el ciberespacio en futuros debates sobre las cuestiones de ciberseguridad en las Naciones Unidas**. Hasta la fecha, esta declaración ha reunido a más de un tercio de los Estados Miembros de la Organización, así como a varios centenares de agentes no estatales de primer orden, en torno a una visión común de los principios que deberían sustentar el comportamiento de los distintos agentes en el ciberespacio.
- **Universalizar el Convenio sobre la Ciberdelincuencia**. Adoptado en noviembre de 2001 para reforzar la cooperación internacional en la materia, este instrumento ha sido ratificado hasta el momento por 63 Estados y ha influido en la legislación nacional de más de dos tercios de los Estados Miembros de las Naciones Unidas.
- **Alentar a los Estados a hacer gala de transparencia**. Esto incluye su estrategia de ciberseguridad, su doctrina sobre la gestión de las crisis cibernéticas y la respuesta a los ataques cibernéticos, y su interpretación de la aplicación del derecho internacional al ciberespacio.
- **Poner en práctica en los marcos regionales o internacionales pertinentes las medidas de confianza específicas para encarar los retos cibernéticos que pudieran haber surgido**.
- **Reforzar las iniciativas y los mecanismos que permitan el intercambio de buenas prácticas y el fortalecimiento de las capacidades**. Esos mecanismos deberían tener por objeto proporcionar a todos los Estados un mecanismo eficaz de ciberseguridad, entre otras cosas mediante:
  - La aplicación de una estrategia de ciberseguridad;
  - La definición de un marco legislativo para promover la ciberseguridad y la lucha contra la ciberdelincuencia;
  - La creación de un centro de respuesta a las emergencias informáticas;
  - El establecimiento de procedimientos de cooperación con el sector privado, incluidas las grandes empresas digitales;

  - La definición de un marco para la protección de las infraestructuras vitales en el ciberespacio.

- **Reconocer a nivel internacional un principio de responsabilidad en materia de seguridad por parte de los actores privados sistémicos**. Esta responsabilidad se extiende a la concepción, la integración, el despliegue y el mantenimiento de sus productos, procesos y servicios digitales, a lo largo de su ciclo de vida y de la cadena de suministro.

Grecia

[Original: inglés]
[15 de mayo de 2019]

En diciembre de 2018, la Asamblea General aprobó una resolución sobre la promoción de un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. En la resolución se pide al Secretario General que recabe las opiniones y evaluaciones de los Estados Miembros sobre: a) los esfuerzos realizados en el plano nacional para fortalecer la seguridad de la información y promover la cooperación internacional en esta esfera; y b) el contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales.

Grecia apoya la opinión consensuada del Grupo de Expertos Gubernamentales de que el derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables también en el ciberespacio y son esenciales para mantener la paz y la estabilidad y promover un entorno abierto, seguro, pacífico y accesible en materia de tecnología de la información y las comunicaciones. Grecia también apoya la continuación del proceso de examen de las normas relativas al comportamiento responsable de los Estados, las medidas de fomento de la confianza y el derecho internacional en el marco de la Primera Comisión de las Naciones Unidas, así como el establecimiento de un nuevo Grupo de Expertos Gubernamentales.

Reconocemos que la naturaleza interconectada y compleja del ciberespacio exige esfuerzos conjuntos de los gobiernos, el sector privado, la sociedad civil, la comunidad técnica, los usuarios y los círculos académicos para hacer frente a los desafíos que se plantean y exhortamos a todas las partes interesadas a que reconozcan y asuman sus responsabilidades específicas para mantener un ciberespacio abierto, libre, seguro y estable.

Reconocemos también el papel de las Naciones Unidas en cuanto a seguir elaborando normas para un comportamiento responsable de los Estados en el ciberespacio y recordamos que los resultados de los debates del Grupo de Expertos Gubernamentales han articulado un conjunto consensuado de normas y recomendaciones, que la Asamblea General ha hecho suyas en repetidas ocasiones, y que los Estados deberían tomar como base para un comportamiento responsable de los Estados en el ciberespacio.

Mediante nuestra participación en organizaciones internacionales como las Naciones Unidas, la Unión Europea, la Organización del Tratado del Atlántico del Norte y la Organización para la Seguridad y la Cooperación en Europa, tratamos de establecer normas y principios universales sobre el comportamiento responsable de los Estados en la utilización del ciberespacio, cooperar, intercambiar experiencias y prácticas óptimas y elaborar conjuntamente medios adecuados para hacer frente a las amenazas y los desafíos relacionados con la ciberseguridad. Nuestro país contribuye en la mayor medida posible a la formulación y aplicación de las decisiones pertinentes

adoptadas en el marco de las organizaciones internacionales con el objetivo de aumentar la cooperación y la transparencia y reducir el riesgo de conflicto.

Reconociendo que la ciberdelincuencia es un problema mundial, Grecia ha firmado y ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como el Tratado de Budapest. Este tratado proporciona un marco importante tanto para la adopción de nuestra legislación nacional como para la cooperación internacional en la lucha contra la ciberdelincuencia. El tratado fue ratificado por la Ley 4411/2016. Asimismo, en el marco de nuestra participación en la Organización para la Seguridad y la Cooperación en Europa, nuestro país también ha firmado el Acuerdo sobre Medidas de Fomento de la Confianza, que tiene por objeto fomentar la cooperación de los Estados Miembros en cuestiones de ciberseguridad, transparencia, estabilidad y reducción del riesgo de enfrentamiento en el ciberespacio.

En el marco de los compromisos de la Unión Europea, Grecia ha incorporado a su legislación nacional la Directiva 1148 relativa a la seguridad de las redes y los sistemas de información, también conocida como Directiva NIS, que incluye medidas para lograr un alto nivel común de seguridad en toda la Unión, mediante la aplicación de medidas de ciberseguridad, la elaboración de una estrategia nacional y el aumento de la cooperación entre los Estados miembros. Como resultado de ello, se refuerza la protección de todas las infraestructuras vitales de nuestro país, al tiempo que se salvaguardan los principios de una sociedad abierta, las libertades constitucionales y los derechos individuales. La Autoridad Nacional de Ciberseguridad, que funciona bajo la supervisión del Ministerio de Política Digital, tiene la responsabilidad general de aplicar la estrategia nacional de ciberseguridad.

Los objetivos clave de nuestra estrategia nacional en materia de ciberseguridad son los siguientes:

- Desarrollar y consolidar un ciberespacio seguro y resistente sobre la base de normas y prácticas nacionales, europeas e internacionales
- Mejorar de manera continua nuestras capacidades de protección contra los ciberataques, haciendo énfasis en las infraestructuras vitales
- Fomentar una fuerte cultura de seguridad pública y privada, explotando el potencial tanto de la comunidad académica como de los agentes públicos y privados
- Mejorar el nivel de la evaluación, el análisis y la prevención de las amenazas para la seguridad de los sistemas e infraestructuras de información
- Establecer un marco eficaz de coordinación y cooperación entre las partes interesadas de los sectores público y privado
- Promover la participación activa del país en las iniciativas internacionales y en las medidas adoptadas por las organizaciones internacionales en relación con la ciberseguridad
- Fomentar la sensibilización entre todos los interesados sociales e informar a los usuarios sobre el uso seguro del ciberespacio
- Adaptar constantemente el marco institucional nacional a los nuevos requerimientos tecnológicos así como a las directrices europeas
- Promover la innovación, la investigación y el desarrollo en materia de seguridad.

Japón

[Original: inglés]
[14 de mayo de 2019]

1. Evaluación general de las cuestiones relacionadas con la seguridad de la información

Los conocimientos, las tecnologías y los servicios en el ciberespacio, como la inteligencia artificial, la Internet de las cosas, el sector tecnofinanciero, los macrodatos y la 5G, se están estableciendo en la sociedad y están dando lugar a innovaciones que están transformando las estructuras existentes en nuestras actividades socioeconómicas y en la vida cotidiana de las personas, y estas transformaciones están produciendo avances en la unificación del ciberespacio y el espacio real. Para poder disfrutar de los beneficios de los conocimientos, las tecnologías y los servicios del ciberespacio, es esencial controlar las incertidumbres latentes que siempre existen en él. Cuando ese control no es posible, existe la posibilidad de que las amenazas relacionadas con la ciberseguridad aumenten rápidamente.

Beneficios del ciberespacio

El número de usuarios de Internet en el mundo está aumentando, al igual que la difusión de la propia Internet. Además, en términos de dispositivos, la tasa de posesión de teléfonos inteligentes personales ha aumentado considerablemente, y la tasa de uso de Internet también está aumentando. La proporción de usuarios de medios sociales también está aumentando, como resultado de lo cual ahora existe un entorno para comunicarse fácilmente en el ciberespacio. La creciente adopción de servicios en el ciberespacio por la sociedad ha promovido no solo la libre circulación de la información, sino también la formación de comunidades diversas y el intercambio de información. También ha habido avances en el ámbito de las actividades financieras, incluidas las compras en línea, el comercio de acciones y las operaciones bancarias en línea, mientras que aparecen frecuentemente nuevos servicios en los ámbitos de sector tecnofinanciero y de la economía compartida, que lideran la innovación. También se ha avanzado en el uso de la tecnología de la información y las comunicaciones en las esferas de la medicina y la enfermería, el bienestar, la educación y otras esferas relacionadas con cuestiones sociales como la disminución de la población en edad de trabajar y el envejecimiento de las comunidades locales.

Amenazas crecientes en el ciberespacio

Si bien la inteligencia artificial, la Internet de las cosas y otras tecnologías y servicios tienen el potencial de aportar muchos beneficios a las personas, siempre existe el riesgo latente de que los proveedores de estas tecnologías y servicios pierdan la capacidad de controlarlos, en cuyo caso pueden causar pérdidas o daños económicos y sociales inconmensurables. A medida que avanza la unificación del ciberespacio y el espacio real, la probabilidad de que esto ocurra aumenta exponencialmente. Además, el ciberespacio es un lugar sin restricciones espaciales ni temporales en el que cualquier persona, en particular los agentes malintencionados, puede hacer un uso indebido y abusar de las nuevas tecnologías de la información y las comunicaciones con facilidad. La propia naturaleza de la tecnología digital permite a los agentes malintencionados copiar y distribuir fácilmente datos e información sensibles, lanzar programas de ataque e incorporar de forma flexible las tecnologías emergentes, como la inteligencia artificial y la cadena de bloqueo, y hacer libre uso de ellas. Por esa razón, los atacantes tienen una ventaja asimétrica sobre los defensores, y se espera que esa ventaja aumente especialmente cuando la formación del defensor depende de las políticas y los sistemas tecnológicos existentes. En vista

de estas condiciones, se han producido ataques dirigidos a la Internet de las cosas, el sector tecnofinanciero, incluyendo las cibermonedas, las infraestructuras vitales y las cadenas de suministro, lo que ha causado pérdidas financieras directas y la interrupción de negocios y servicios, además de la habitual violación de datos, y ha servido para amenazar la seguridad y la protección del desarrollo sostenible de las actividades socioeconómicas y la vida de las personas. También ha habido incidentes masivos de los que se sospecha que han sido patrocinados por un Estado. Además, existe la preocupación de que la credibilidad de la infraestructura de la información pueda verse afectada si el gobierno de algunos países controla y gestiona el ciberespacio desde una posición superior. Se cree que a medida que el ciberespacio se vaya unificando con el espacio real, aumentarán las preocupaciones por los posibles intentos de abordar las debilidades de la Internet de las cosas, las cadenas de suministro y la innovación abierta, y que se producirán comportamientos no deseados en estos sistemas. Esto podría afectar seriamente no solo a los organismos gubernamentales y a los operadores de infraestructuras vitales, sino también a otras empresas e incluso a particulares.

Adhesión a la posición básica sobre el ciberespacio

A fin de seguir disuadiendo las actividades de agentes malintencionados y garantizar la seguridad y los derechos de las personas, el Japón mantiene, como sus opciones, los medios políticos, económicos, tecnológicos, jurídicos, diplomáticos y todos los demás medios viables y eficaces. El Japón se adhiere a los cinco principios para elaborar y aplicar medidas de ciberseguridad, que son: i) la garantía de la libre circulación de la información; ii) el estado de derecho; iii) la apertura; iv) la autonomía; y v) la colaboración entre múltiples partes interesadas.

i) Garantía de la libre circulación de la información

Para lograr el desarrollo sostenible del ciberespacio como lugar de creación e innovación, es imperativo construir y mantener un mundo en que la información transmitida llegue al destinatario previsto sin que haya sido censurada injustamente o modificada ilegalmente en el camino. También deben garantizarse las consideraciones de privacidad. Como condición básica para la libre circulación de la información en el ciberespacio, es necesario que la moral y el sentido común no atenten contra los derechos e intereses de los demás.

ii) El estado de derecho

A medida que avanza la unificación del ciberespacio y el espacio real, el estado de derecho también debería mantenerse en el ciberespacio de la misma manera que en el espacio real. En el ciberespacio se aplican diversas reglas y normas nacionales, incluidas las leyes y reglamentos nacionales. Del mismo modo, el derecho internacional vigente también se aplica en el ciberespacio. La aplicación del derecho internacional vigente y la elaboración de normas siguen siendo esenciales para el desarrollo sostenible del ciberespacio como espacio seguro y fiable.

iii) Apertura

Para lograr el desarrollo sostenible del ciberespacio como espacio de generación de nuevos valores, el ciberespacio debe estar abierto a todos los actores sin restringir las posibilidades de vincular ideas y conocimientos diversos. El Japón se adhiere a la posición de que el ciberespacio no debe estar dominado exclusivamente por un pequeño grupo de actores.

iv) Autonomía

El ciberespacio se ha desarrollado gracias a las iniciativas autónomas de múltiples partes interesadas. Es inapropiado e imposible que un Estado asuma toda la función de mantener el orden para que el ciberespacio se desarrolle de manera sostenible como un espacio en que coexistan el orden y la creatividad. El único enfoque para mantener el orden y disuadir y abordar el comportamiento de los agentes malintencionados consiste en que los diversos sistemas sociales funcionen de manera autónoma. El Japón promoverá este enfoque.

v) Colaboración entre múltiples partes interesadas

El ciberespacio es un mundo multidimensional establecido a través de las actividades de múltiples partes interesadas, incluidos el Estado, los gobiernos locales, los operadores de infraestructuras vitales, las empresas relacionadas con el ciberespacio y de otro tipo, las instituciones educativas y de investigación, y los particulares. Para lograr el desarrollo sostenible del ciberespacio, es necesario que todos los actores cumplan conscientemente sus respectivas funciones y responsabilidades. Esto requerirá coordinación y colaboración además de esfuerzos individuales. Los Estados desempeñan el papel principal en la promoción de esta coordinación y colaboración y promoverán medidas que permitan el cumplimiento de esas funciones.

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

Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información

En el Japón se han preparado las bases jurídicas para la utilización de los datos, incluida la Ley Básica sobre el Fomento de la Utilización de Datos de los Sectores Público y Privado, la Ley Enmendada sobre la Protección de la Información Personal, etc. El Gobierno también ha adoptado una política de creación de una sociedad antropocéntrica que logre el desarrollo económico y la solución de los problemas sociales mediante un alto nivel de integración del ciberespacio con el espacio real. En estas circunstancias, las enormes cantidades de datos generados por los sensores y dispositivos en el espacio real se están acumulando y analizando actualmente en el ciberespacio. Además, se puede observar que el suministro en el espacio real de nuevos productos y servicios que añaden valor mediante la utilización de datos está emergiendo y desarrollándose cíclicamente en numerosos ámbitos. El ciberespacio y el espacio real han dejado de existir como entidades independientes, sino que son entidades que interactúan entre sí, de modo que ya no pueden considerarse separadas. Por lo tanto, los dos espacios deben ser vistos como una entidad orgánica única en continua evolución.

La unificación del ciberespacio y el espacio real aumenta considerablemente las posibilidades de proporcionar abundancia a la sociedad. Al mismo tiempo, también aumenta las posibilidades de que agentes malintencionados hagan mal uso del ciberespacio. Se espera que el riesgo de pérdida o daño económico y social en el espacio real aumente y se acelere exponencialmente. En estas circunstancias, debe garantizarse la seguridad del ciberespacio, que constituye la base de la sociedad económica, y, al mismo tiempo, su evolución y desarrollo autónomos y sostenidos a fin de lograr un progreso y una riqueza sostenibles para la sociedad.

Recientemente, ha habido una tendencia en algunos países a responder a las ciberamenazas haciendo hincapié en la gestión y el control por parte del Estado desde una posición dominante. Sin embargo, el fortalecimiento de la gestión y el control del ciberespacio por parte del Estado tienen el efecto de obstaculizar la posibilidad de un

desarrollo autónomo y sostenible. Por consiguiente, debe respetarse el ciberespacio actual, que se ha desarrollado mediante las iniciativas autónomas de todas las partes interesadas, y debe garantizarse la ciberseguridad mediante iniciativas de colaboración y cooperación con esas partes interesadas. Sobre la base de este entendimiento, consciente de la situación que debe perseguirse para 2020 y años posteriores y teniendo en cuenta la celebración de eventos internacionales como los Juegos de la XXXII Olimpiada y los Juegos Paralímpicos de Tokio en 2020 (en lo sucesivo “los Juegos de Tokio 2020”), el Japón no escatimará esfuerzos en relación con las medidas de ciberseguridad, aclarando la visión básica de la ciberseguridad, identificando los nuevos problemas que deben abordarse y adoptando medidas de rápida aplicación.

Esfuerzos realizados en el plano nacional para promover la cooperación internacional

En vista de que los efectos de los incidentes en el ciberespacio pueden extenderse fácilmente más allá de las fronteras nacionales, los ciberincidentes en el extranjero siempre pueden afectar al Japón. El Japón cooperará y colaborará con los gobiernos y el sector privado de todo el mundo para garantizar la seguridad del ciberespacio y trabajar en pro de la paz y la estabilidad de la comunidad internacional y la seguridad nacional del Japón. Con este fin, el Gobierno contribuirá activamente a diversos debates internacionales y trabajará para compartir información y desarrollar un entendimiento común respecto de las cuestiones relacionadas con la cibernética. El Gobierno también compartirá conocimientos especializados con países extranjeros, promoverá la cooperación y la colaboración específicas y tomará medidas.

En lo que respecta al intercambio de conocimientos especializados y la política de coordinación, el Gobierno trabajará mediante diálogos bilaterales y conferencias internacionales sobre ciberseguridad para intercambiar información sobre políticas, estrategias y sistemas de ciberseguridad a fin de responder, y utilizará esos conocimientos en la planificación de la política de ciberseguridad del Japón. También reforzaremos nuestra cooperación y colaboración en materia de política de ciberseguridad con socios estratégicos que comparten con nosotros los principios básicos de la ciberseguridad.

En cuanto a la colaboración internacional para dar respuesta a incidentes, el Gobierno compartirá información sobre ciberataques y amenazas y fortalecerá la cooperación entre los equipos informáticos de respuesta de emergencia para facilitar una respuesta coordinada cuando se produzcan incidentes. El Gobierno también trabajará para mejorar la capacidad de respuesta coordinada mediante la capacitación conjunta y la participación en ejercicios cibernéticos internacionales. Además, el Gobierno responderá adecuadamente en caso de incidentes mediante la colaboración internacional adecuada.

A la luz de los aspectos diplomáticos de la cooperación internacional relacionada con el ciberespacio, nuestros compromisos se sustentan en tres pilares: el estado de derecho, las medidas de fomento de la confianza y la creación de capacidad en el ciberespacio.

- La promoción del estado de derecho es importante para la paz y la estabilidad internacionales y la seguridad nacional del Japón. La posición del Japón es que el derecho internacional vigente, incluida la Carta de las Naciones Unidas, se aplica también al ciberespacio, y el Japón contribuirá de manera proactiva a los debates sobre las aplicaciones individuales y específicas del derecho internacional vigente y la elaboración de normas y su universalización. Con respecto a las medidas contra la ciberdelincuencia, el Organismo Nacional de Policía y otros ministerios y organismos competentes colaborarán para seguir

promoviendo las asociaciones internacionales mediante la cooperación internacional en materia de investigación y el intercambio de información con las organizaciones internacionales, los organismos encargados de hacer cumplir la ley y los organismos de información sobre la seguridad de otros países, aprovechando determinados marcos como la Convención sobre la Ciberdelincuencia, los tratados de asistencia judicial recíproca y la Organización Internacional de Policía Criminal (INTERPOL).

- El Japón trabajará para fomentar la confianza entre los Estados a fin de evitar que se produzcan circunstancias imprevistas y se deteriore la situación causada por los ciberataques. Debido al anonimato y al carácter secreto de los ciberataques, existe el riesgo de que estos aumenten involuntariamente las tensiones entre los Estados y empeoren la situación. Para evitar esos enfrentamientos accidentales e innecesarios, es importante crear canales de comunicación internacional en tiempos de paz como preparación para la ocurrencia de incidentes que se extiendan más allá de las fronteras nacionales. También es necesario aumentar la transparencia y fomentar la confianza entre los Estados mediante el intercambio proactivo de información y los diálogos sobre políticas en consultas bilaterales y multilaterales. El Gobierno también cooperará con otros Estados para considerar la posibilidad de establecer un mecanismo de coordinación de las cuestiones relativas al ciberespacio. En este contexto, el Japón promueve con entusiasmo las medidas de fomento de la confianza, entre otras cosas, mediante el inicio del establecimiento de la reunión entre períodos de sesiones del foro regional de la Asociación de Naciones del Asia Sudoriental (ASEAN) en la esfera de la seguridad cibernética, cuya copresidencia ocupa, sin dejar de prestar asistencia constante al fomento de la capacidad, principalmente en la región de Asia y el Pacífico.

- En cuanto al fomento de la capacidad, a medida que se ha profundizado la interdependencia a través de las fronteras, el Japón no puede garantizar por sí solo la paz y la estabilidad. La coordinación mundial para reducir y eliminar las vulnerabilidades de la ciberseguridad es esencial para garantizar la seguridad nacional del Japón. Desde este punto de vista, la asistencia a la creación de capacidades en otros Estados garantiza la estabilidad de la vida de los residentes japoneses y las actividades de las empresas japonesas en otros países que dependen de las infraestructuras vitales en esos Estados, así como el desarrollo racional de la utilización del ciberespacio en esos Estados. Al mismo tiempo, también está directamente relacionado con la seguridad de todo el ciberespacio y contribuye a mejorar el entorno de seguridad para todo el mundo, en particular el Japón. Además, en la esfera de la ciberdelincuencia, el Japón es una de las pocas partes no europeas en el Convenio sobre la Ciberdelincuencia y desempeña un papel positivo en la promoción del Convenio, que constituye un importante marco jurídico para combatir la ciberdelincuencia, mediante la prestación de asistencia para la creación de capacidad en la región de Asia.

3. Conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones

El Japón apoya los acuerdos consensuados de los Grupos de Expertos Gubernamentales anteriores en el sentido de que el derecho internacional vigente se aplica en el ciberespacio. Hemos visto que el debate sobre la elaboración de conductas normativas, la puesta en práctica de medidas de fomento de la confianza y la creación de capacidad son los enfoques fundamentales para configurar una conducta responsable de los Estados en el ciberespacio. En particular, el Japón reconoce que la aplicación de normas voluntarias y no vinculantes sobre la conducta responsable de los Estados en el ciberespacio, a las que se hace referencia en el informe de 2015 del

Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, debe ser la base para garantizar la estabilidad y la previsibilidad internacionales, así como para los debates futuros sobre esta cuestión. En este sentido, creemos que cualquier intento de concertar nuevos tratados amplios o instrumentos similares no mejoraría positivamente la ciberseguridad en la actualidad.

4. Medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial

Como Estado responsable, el Japón, sin dejar de promover la coordinación de la comunidad internacional con los marcos regionales pertinentes sobre la base del derecho internacional vigente y de todos los conceptos identificados por conducto del Grupo de Expertos Gubernamentales, considera que la elaboración de un entendimiento común de las normas voluntarias y no vinculantes sobre la conducta responsable de los Estados y la aplicación de esas normas contribuirán al fortalecimiento de la seguridad internacional.

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

El Japón considera que es eficaz y significativo que todos los Estados tengan en cuenta los siguientes conceptos identificados por el Grupo de Expertos Gubernamentales:

Influencia de las ciberactividades maliciosas en la comunidad internacional

Para incorporar con flexibilidad el rápido desarrollo de las tecnologías de la información y las comunicaciones en nuestras vidas y evitar los daños derivados de ciberactividades maliciosas, debemos reconocer la importancia de prever las amenazas existentes y potenciales en el ciberespacio y la forma en que la comunidad internacional podría verse afectada por ellas.

Aplicación de normas voluntarias y no vinculantes sobre la conducta responsable de los Estados

Para reducir al mínimo los efectos de las ciberactividades maliciosas y disuadir a quienes los cometan, debemos recordar la importancia del informe consensuado del Grupo de Expertos Gubernamentales, incluidas las normas voluntarias y no vinculantes sobre la conducta responsable de los Estados a las que se hace referencia en él. Deberíamos profundizar nuestros debates, en colaboración con las organizaciones regionales pertinentes, para aprovechar de manera práctica y eficaz estos valiosos esfuerzos.

Promoción de la aplicación de normas voluntarias y no vinculantes sobre la conducta responsable de los Estados y de la cooperación para la adopción de medidas pertinentes de fomento de la confianza y la creación de capacidad

Para seguir intensificando los esfuerzos de cada Estado por desarrollar y mantener un ciberespacio libre, justo y seguro en el contexto de la seguridad internacional, debemos reafirmar que todas las naciones tienen la firme voluntad de eliminar los agujeros de seguridad en el ciberespacio y prevenir la ciberdelincuencia y otros actos malintencionados. En este contexto, los miembros del grupo deberían dedicarse sistemáticamente a alentar a todos los Estados a que apliquen de manera constante las normas voluntarias y no vinculantes sobre la conducta responsable de los Estados, incluidas las medidas de fomento de la confianza y la cooperación para ayudar a fomentar la capacidad nacional de aplicar las normas y recomendaciones

voluntarias y no vinculantes antes mencionadas, incluso mediante el proceso del próximo Grupo de Expertos Gubernamentales y del grupo de trabajo de composición abierta.

Singapur

[Original: inglés]
[13 de mayo de 2019]

Singapur reconoce que las amenazas a un ciberespacio abierto, seguro y pacífico son cada vez más sofisticadas, transfronterizas y asimétricas. Como Estado pequeño y con un alto nivel de interconexión que ha sido objeto de varios ciberataques, Singapur está firmemente comprometido con el establecimiento de un orden internacional basado en normas en el ciberespacio. Esto servirá de base para el fortalecimiento de la confianza entre los Estados miembros y permitirá el progreso económico y social. Para aprovechar plenamente los beneficios de las tecnologías digitales, la comunidad internacional debe crear un ciberespacio seguro, fiable y abierto, basado en el derecho internacional aplicable al ciberespacio, normas bien definidas de comportamiento responsable de los Estados, medidas sólidas de fomento de la confianza y creación de capacidades coordinadas. Colectivamente, estas tres corrientes crean un bucle triangular que se refuerza mutuamente y que hará posible la creación de un ciberespacio seguro y resistente. Es importante que los iniciativas para examinar 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, grandes o pequeños, tienen voz. Singapur está comprometido con este proceso.

Singapur acoge con beneplácito el establecimiento del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y la decisión de convocar un grupo de trabajo de composición abierta. Singapur considera que la labor del Grupo de Expertos Gubernamentales y del grupo de trabajo puede y debe ser complementaria. Es importante que los principales actores trabajen juntos, en un espíritu de consenso, respeto mutuo y confianza mutua. Singapur es optimista en cuanto a que ambas plataformas puedan complementarse mutuamente de manera positiva y se ha comprometido a contribuir de manera constructiva a ambos procesos.

A nivel regional, Singapur colaboró con otros Estados miembros de la Asociación de Naciones del Asia Sudoriental (ASEAN) para publicar la primera declaración de los dirigentes de la ASEAN sobre cooperación en materia de ciberseguridad, durante la 32ª Cumbre de la ASEAN, celebrada en abril de 2018. En la declaración, los dirigentes de la ASEAN reafirmaron la necesidad de establecer un orden internacional basado en normas en el ciberespacio. También encomendaron a los ministros competentes la tarea de determinar un mecanismo o plataforma adecuados para coordinar las políticas de ciberseguridad, la diplomacia, la cooperación y las actividades técnicas y de fomento de la capacidad en toda la ASEAN, así como la elaboración de una lista concreta de normas voluntarias y prácticas de comportamiento de los Estados en el ciberespacio que la ASEAN pudiera adoptar en el futuro. Sobre la base de la declaración de los dirigentes, en septiembre de 2018, los participantes en la tercera Conferencia Ministerial de la ASEAN sobre Ciberseguridad, celebrada en Singapur, acordaron suscribir en principio las 11 normas del informe de 2015 del Grupo de Expertos Gubernamentales (A/70/174), así como centrarse en el fomento de la capacidad regional para aplicar esas normas.

El fomento de la capacidad es esencial para asegurar que los Estados desarrollen la capacidad de aplicar con éxito las reglas y normas de comportamiento. Singapur cuenta con un programa de capacidad cibernética de la ASEAN de 10 millones de

dólares de Singapur, un programa modular, multidisciplinario y con múltiples partes interesadas que se centra en la creación de capacidad en los países de la ASEAN en materia de políticas, estrategias y cuestiones técnicas relacionadas con la cibernética. Desde su creación en 2016, 160 funcionarios de la ASEAN han recibido capacitación en el marco del Programa. Singapur también se ha asociado con la Oficina de Asuntos de Desarme para elaborar un curso insignia de capacitación en línea a fin de promover la comprensión y la aplicación de los acuerdos alcanzados por el Grupo de Expertos Gubernamentales. También colaborará con la Oficina en un programa cibernético de las Naciones Unidas y Singapur para crear conciencia sobre las normas cibernéticas y la planificación de políticas en relación con situaciones cibernéticas en los Estados miembros de la ASEAN. Como extensión del Programa de Fomento de la Capacidad Cibernética de los Miembros de la ASEAN, Singapur pondrá en marcha en 2019 el Centro de Excelencia de la ASEAN y Singapur en materia de Ciberseguridad, con un presupuesto de 30 millones de dólares de Singapur, a fin de seguir fomentando la formulación de políticas, el desarrollo de estrategias y la capacidad técnica y operacional en materia de ciberseguridad de los países de la ASEAN. El Centro será abierto e inclusivo, y los Estados miembros de la ASEAN pueden aprovecharlo para colaborar más estrechamente con los asociados internacionales.

En el plano nacional, Singapur ha realizado importantes avances en el fortalecimiento de la ciberseguridad de sus sistemas y redes en los tres frentes siguientes, a saber, la creación de una infraestructura resistente, la creación de un ciberespacio más seguro y el desarrollo de un ecosistema de ciberseguridad dinámico:

a) *Construir una infraestructura resiliente.* Las ciberamenazas transfronterizas están haciendo peligrar cada vez más la infraestructura crítica de los países. Esto es especialmente cierto en los casos de infraestructura de información supranacional, como en los sectores financiero, marítimo, de telecomunicaciones y de aviación, donde las consecuencias de un ciberataque exitoso podrían extenderse más allá de las fronteras nacionales y afectar a los centros interconectados de todo el mundo. Un acontecimiento clave en 2018 fue la aprobación y aplicación de la Ley de Ciberseguridad, que estableció un marco jurídico para la supervisión y el mantenimiento de la ciberseguridad nacional en Singapur. En la ley se hace hincapié en la protección proactiva contra ataques cibernéticos a la infraestructura de información crítica, es decir, a los ordenadores o sistemas informáticos que respaldan la prestación de servicios esenciales. Esta protección se logra mediante la imposición de obligaciones legales a los propietarios de dicha infraestructura para, entre otras cosas, hacer lo siguiente: i) establecer mecanismos para detectar amenazas e incidentes de ciberseguridad y denunciar tales incidentes; ii) realizar periódicamente evaluaciones de riesgos y auditorías de las infraestructuras críticas de información; y iii) participar en ejercicios de ciberseguridad realizados por la autoridad nacional de ciberseguridad. Además de reforzar la protección de esa infraestructura, la autoridad nacional de ciberseguridad también está autorizada, en virtud de la Ley, a prevenir e investigar las amenazas y los incidentes relacionados con la ciberseguridad y responder ante ellos;

b) *Crear un ciberespacio más seguro.* En enero de 2019, Singapur alcanzó la condición de nación que autoriza la expedición de certificados en virtud del acuerdo de reconocimiento de criterios comunes, que es un acuerdo internacional para el reconocimiento mutuo de los certificados de criterios comunes en 30 naciones. Los criterios comunes son una norma técnica aplicada a la evaluación y certificación de los productos de seguridad de la tecnología de la información y son ampliamente adoptados tanto por los Gobiernos como por la industria. Singapur es ahora uno de los 18 de los 30 países que autorizan la expedición de certificados en virtud del acuerdo. Como tal, se permite a Singapur certificar los productos de seguridad de la tecnología de la información a nivel local, contribuyendo así a mejorar la calidad de

los productos de ciberseguridad de las pequeñas y medianas empresas de Singapur mediante la comparación con las normas internacionales de seguridad;

c) *Desarrollar un ecosistema vibrante de ciberseguridad.* Singapur reconoce que el fortalecimiento de la ciberseguridad implica la construcción del ecosistema cibernético y el fomento de la innovación en la industria. Con este fin, Singapur puso en marcha su primer centro empresarial integrado de ciberseguridad en marzo de 2018, denominado Innovation Cybersecurity Ecosystem at Block71 (Ecosistema de ciberseguridad de la innovación en el bloque 71), cuyo objetivo es fortalecer el creciente ecosistema de ciberseguridad de Singapur mediante la atracción y el desarrollo de competencias y tecnologías profundas que ayuden a mitigar los riesgos de la ciberseguridad, que aumentan rápidamente. También ayuda a desarrollar nuevas empresas de ciberseguridad en todo el mundo, a través de una serie de programas diseñados para apoyar a los empresarios, desde la creación de ideas hasta la aceleración y ampliación de las nuevas empresas de ciberseguridad para el mercado mundial.

Turquía

[Original: inglés]
[10 de mayo de 2019]

La tecnología de la información y las comunicaciones (TIC) se ha convertido en parte esencial de la sociedad y la economía. Se utiliza en una amplia red que incluye al sector público, el sector privado, infraestructuras esenciales y los individuos, y se ha generalizado en nuestro país y en el mundo. Como resultado de ello, las TIC desempeñan un papel importante para el crecimiento y el desarrollo sostenibles. Sin embargo, cuanto más utilizamos la tecnología, más dependemos de ella y somos más propensos a los riesgos que conlleva. Las personas, las empresas, las infraestructuras críticas y los Estados se enfrentan a graves problemas debido a las ciberamenazas.

La difusión de la tecnología en todas las dimensiones de nuestra vida nos ha llevado a una nueva etapa con respecto a los riesgos asociados en el contexto de la ciberseguridad. Garantizar la ciberseguridad no es solo una necesidad para hacer frente a las amenazas en zonas de gran intensidad tecnológica, sino también un factor importante que afecta a la prosperidad y la seguridad nacional de los países debido a los riesgos que plantea para el curso de la vida social y económica.

Las deficiencias en materia de seguridad de las TIC pueden hacer que esos sistemas queden fuera de servicio o sean explotados, o pueden provocar la pérdida de vidas humanas, pérdidas económicas a gran escala, perturbaciones del orden público o comprometer la seguridad nacional.

Turquía centra su labor en la adopción de las medidas necesarias para mejorar la ciberseguridad nacional y ha venido aplicando la estrategia y el plan de acción nacionales de ciberseguridad, que abarca el período comprendido entre 2016 y 2019, con la misión de establecer la ciberseguridad nacional, formular y coordinar políticas eficientes y sostenibles y llevar a la práctica esas políticas. El Ministerio de Transporte e Infraestructura es el organismo responsable de la elaboración de políticas y estrategias y de planes de acción sobre ciberseguridad nacional en Turquía. En este contexto, la estrategia y el plan de acción nacionales de ciberseguridad se elaboraron con la participación de todas las partes interesadas en grupos de estudios, bajo la coordinación del Ministerio de Transporte e Infraestructura.

La estrategia y el plan de acción tienen dos objetivos principales: en primer lugar, que todas las partes interesadas reconozcan y comprendan que la ciberseguridad es parte integrante de la seguridad nacional; y en segundo lugar, que se adquiera la

competencia que permita tomar las precauciones administrativas y tecnológicas necesarias para mantener la seguridad absoluta de todos los sistemas y partes interesadas en el ciberespacio nacional.

Cada una de las actividades de la estrategia y el plan de acción ha sido llevada a cabo por el Ministerio de Transporte e Infraestructura y organismos conexos, y el Ministerio ha supervisado todos los avances de cada una de ellas.

Además, la Autoridad de Tecnologías de la Información y la Comunicación ha sido el equipo informático de respuesta de emergencia a nivel nacional de Turquía desde 2013. Es responsable de todas las funciones reguladoras relativas a las comunicaciones electrónicas y los servicios postales en Turquía. Además, se le ha otorgado la facultad de adoptar las medidas necesarias para luchar contra los ciberataques a fin de garantizar la ciberseguridad nacional. El Equipo actúa como centro de coordinación a nivel nacional para identificar las amenazas contra la ciberseguridad del país, tomar medidas para reducir o eliminar el impacto de los posibles ciberataques y compartir información con actores definidos. Proporciona coordinación con todas las partes interesadas, como instituciones públicas o privadas y particulares, para la detección y eliminación de ciberamenazas. Sus principales áreas de interés en materia de ciberseguridad son:

- El desarrollo de la capacidad cibernética
- Las medidas tecnológicas
- La recopilación y difusión de información sobre amenazas
- La protección de las infraestructuras vitales

En el ámbito de la creación de capacidad, las actividades incluyen los recursos humanos, la formación y los preparativos. En el marco de estas actividades, organizamos certámenes de “captura de la bandera” sobre ciberseguridad. Creemos que los recursos humanos son uno de los factores más importantes de la ciberseguridad. En el contexto del equipo informático de respuesta de emergencia a nivel nacional, llevamos a cabo proyectos clave para el desarrollo de la capacidad. En este sentido, organizamos formación en ciberseguridad para los equipos informáticos institucionales de respuesta de emergencia de diversos sectores críticos, como la energía, la salud y las instituciones públicas. También realizamos capacitación práctica y concursos para estudiantes y graduados. En los últimos dos años, más de 2.500 personas han asistido a nuestros programas de formación en ciberseguridad.

También hemos establecido un laboratorio de alcance cibernético con el fin de mejorar nuestros programas de formación y ofrecer más oportunidades para las actividades prácticas. El laboratorio también es beneficioso para medir el nivel de experiencia y ofrece un programa de certificación para los asistentes.

Nuestros estudios relacionados con las medidas tecnológicas incluyen la detección temprana, las alarmas y las actividades de alerta. Para ello, hemos desarrollado algunos sistemas de detección y prevención. Estos sistemas desempeñan un papel fundamental en el aumento del nivel de ciberseguridad nacional en el país al proporcionar visibilidad y detectar los centros de mando y control de las redes zombis (*botnets*) y los programas maliciosos.

En el ámbito del enfoque de Turquía para mejorar la ciberseguridad, la información sobre las amenazas cibernéticas es otra de las principales áreas de interés que hay que subrayar. En este contexto, trabajamos en coordinación con diversas partes, como agentes de Internet, organizaciones internacionales, autoridades judiciales, centros de investigación y empresas privadas. Además, se han creado equipos informáticos sectoriales de respuesta de emergencia para infraestructuras

críticas y más de 1.000 equipos informáticos institucionales de respuesta de emergencia en instituciones públicas y privadas.

Además, dado que el ciberespacio es un campo sin fronteras, es difícil para una parte garantizar por sí misma su ciberseguridad. Se trata de una cuestión interdisciplinaria y de múltiples partes interesadas. Trabajamos con los usuarios, el sector privado, las organizaciones no gubernamentales, el mundo académico y las contrapartes internacionales para luchar contra las ciberamenazas. Por ejemplo, el equipo informático de respuesta de emergencia de Turquía recibe notificaciones cibernéticas de varios equipos informáticos nacionales de respuesta de emergencia e informa a las partes pertinentes para que tomen las medidas necesarias. También envía información sobre ciberamenazas y comparte información con otros equipos informáticos de respuesta de emergencia nacionales y organizaciones internacionales.

Desde una perspectiva de la seguridad en Internet, en 2017 se creó el Centro para una Internet Segura en el marco de la Autoridad de Tecnologías de la Información y las Comunicaciones, con el fin de aumentar la concienciación sobre el uso adecuado y seguro de Internet.

Se puso en marcha la línea de ayuda por Internet y un sitio web seguro, donde las familias pueden encontrar consejos para el uso eficiente de Internet. Además, el "camión de Internet más seguro", equipado con herramientas de TIC, se ha puesto a disposición de los niños y jóvenes que tienen acceso limitado a las TIC. El camión proporciona una plataforma para que las personas puedan experimentar la tecnología de cerca y ayuda a concienciar sobre el uso seguro y consciente de Internet a los niños que interactúan más con Internet y la tecnología.

La Autoridad organiza anualmente una actividad con motivo del Día de Internet Segura. El tema principal en 2018 fue "Crear, conectar y compartir el respeto: una Internet mejor empieza por ti". La Autoridad y la Universidad Bahçeşehir lanzaron un concurso de juegos de mesa para alentar a los jóvenes de 12 a 18 años a diseñar un juego relacionado con el tema internacional. A lo largo del concurso se recibieron muchos diseños de juegos y los ganadores fueron premiados. Durante este evento, Facebook y Google realizaron talleres para estudiantes sobre juegos digitales y una Internet más segura.

Además, la Autoridad firmó acuerdos con el Ministerio de Familia y Políticas Sociales, la Asociación de Proveedores de Acceso y el Ministerio de Educación en relación con las actividades de sensibilización y formación de instructores sobre el uso consciente y seguro de las TIC e Internet. El contenido de la formación se incluyó en los módulos de educación a distancia y se puso a disposición de todos los profesores que trabajan en el sistema del Ministerio de Educación. Con este servicio de educación a distancia, hasta ahora se ha capacitado a maestros y a miles de estudiantes.

Además, al proporcionar y mantener la seguridad del ciberespacio, no solo la coordinación nacional sino también la cooperación internacional, el intercambio de información y el fomento de la confianza desempeñan un papel crucial.

A continuación se exponen los trabajos y estudios pertinentes realizados en Turquía sobre el alcance de las medidas de fomento de la confianza mencionadas en el informe de 2015 del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (A/70/174) y el concepto de comportamiento responsable de los Estados definido en el informe.

En consonancia con la difusión del uso de las TIC entre las personas, la información o los datos personales se han convertido en un objetivo atractivo para los atacantes cibernéticos. En el contexto de los derechos y libertades fundamentales de

las personas, la protección de la información y los datos personales también ha pasado a ser una preocupación importante.

Junto con la transparencia, la rendición de cuentas y los valores éticos en el entorno cibernético, todas las partes interesadas en Turquía velan por el principio del estado de derecho, los derechos humanos y las libertades fundamentales y la protección de la intimidad, al tiempo que trabajan para garantizar la seguridad del ciberespacio.

En este sentido, el 7 de abril de 2016 se publicó en la Gaceta Oficial núm. 29681 y entró en vigor la Ley núm. 6698 de protección de datos personales. La ley tiene por objeto proteger los derechos y libertades fundamentales de las personas, en particular el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, y definir las obligaciones, los principios y los procedimientos que vinculan a las personas físicas o jurídicas que tratan datos personales.

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. Por consiguiente, Turquía trata de garantizar la ciberseguridad mediante el intercambio de información e ideas en una amplia gama de ámbitos con diversos países y organizaciones sobre la formulación de políticas, el fomento de la capacidad y el intercambio de información.

Dado que el ciberespacio es un campo sin fronteras, es necesario fomentar la cooperación internacional para luchar contra las amenazas cibernéticas. Por ello, Turquía sigue de cerca y participa periódicamente en estudios internacionales sobre ciberseguridad en las Naciones Unidas, la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea, la Organización para la Seguridad y la Cooperación en Europa (OSCE) y otras organizaciones e instituciones internacionales.

Además, con el objetivo de garantizar la ciberseguridad se han establecido acuerdos bilaterales con diversos Estados. El Ministerio de Transporte e Infraestructura, la Autoridad de Tecnologías de la Información y las Comunicaciones y el equipo informático de respuesta de emergencia de Turquía han firmado memorandos de entendimiento sobre ciberseguridad con algunos Estados, como Georgia, Rusia, Kirguistán, Serbia, Bosnia y Herzegovina, Croacia y Grecia.

El memorando de entendimiento que describe la cooperación entre la OTAN y sus aliados es aprobado por el Comité de Ciberdefensa de la OTAN, que tiene en cuenta las opiniones de nuestro Estado, y es firmado por la OTAN y el Ministerio de Defensa de la República de Turquía. Se han establecido puntos de contacto y se están realizando trabajos conexos en el marco del memorando de entendimiento.

Se sigue el trabajo del Comité de Planificación de Emergencias Civiles de la OTAN y del Grupo de Recursos Industriales y Servicios de Comunicaciones. Además, Turquía es miembro desde 2015 del centro de conocimientos, el centro de estudio e instalaciones de formación acreditados por la OTAN, el Centro de Excelencia de Cooperación en Ciberdefensa, en calidad de país patrocinador.

Turquía participa en las reuniones de la Organización de Cooperación y Desarrollo Económicos sobre seguridad y privacidad y contribuye a ellas, así como en el grupo de trabajo oficioso de la OSCE sobre ciberseguridad.

Se realiza un seguimiento de las reuniones del Centro Regional de Asistencia para la Verificación y Aplicación de Medidas de Control de Armamentos y se ha ido desarrollando la cooperación en diversas cuestiones. El objetivo estratégico del Centro es mejorar la elaboración de estrategias nacionales de seguridad mediante el fomento de la cooperación regional en materia de seguridad y la interacción eficaz para hacer frente de manera sostenible a los nuevos problemas de seguridad, como la

ciberseguridad y otras formas de amenazas transnacionales, como el terrorismo, la proliferación de armas de destrucción en masa, el tráfico ilícito, la delincuencia organizada, la seguridad y la gestión de las fronteras y el cambio climático, al tiempo que se prestará especial atención a todas las nuevas amenazas a la seguridad que se deriven de ellas.

Turquía participa en los esfuerzos por desarrollar la cooperación internacional. El Equipo Informático de Respuesta de Emergencia de Turquía es miembro del Foro de Equipos de Seguridad y Respuesta a Incidentes, del servicio de Introductores de Confianza, de la Alianza Multilateral Internacional contra las Ciberamenazas de la Unión Internacional de Telecomunicaciones (UIT), de la plataforma de intercambio de información sobre programas maliciosos de la OTAN y de la Alianza de Ciberseguridad para el Progreso Mutuo, y trata de cooperar en la mayor medida posible para mejorar la información sobre ciberseguridad y compartir conocimientos especializados e información sobre las amenazas a nivel internacional.

Los ejercicios de ciberseguridad son otra actividad importante para la cooperación y la preparación. Estos tipos 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. En este contexto, se realizaron ejercicios nacionales de ciberseguridad en 2011, 2012, 2013 y 2017 en coordinación con el Ministerio de Transporte e Infraestructura. Con la participación de 19 países, el ejercicio internacional de escudo cibernético se completó con éxito en Estambul, con la cooperación de la UIT y su Alianza Multilateral Internacional contra las Ciberamenazas, los días 15 y 16 de mayo de 2014.

Turquía participa regularmente en ejercicios internacionales sobre ciberseguridad y contribuye a su realización, concretamente la Coalición Cibernética de la OTAN, el ejercicio Locked Shields (Escudos Bloqueados) de la OTAN y el Ejercicio de Gestión de Crisis de la OTAN.

En vista de que el ciberespacio no tiene fronteras, las fuentes y los objetivos de los ciberataques pueden encontrarse en diferentes países, incluso en países aliados. Un centro de mando y control puede estar en un país y su objetivo en otro. Por esta razón, el intercambio de información sobre ciberataques y ciberdelincuentes desempeña un papel crucial en la lucha contra las ciberamenazas a escala mundial.

El Convenio sobre la Ciberdelincuencia, el único convenio vinculante, elaborado por el Consejo de Europa, se abrió a la firma en Budapest en 2001 y entró en vigor en 2004. Turquía lo firmó en Estrasburgo en 2010. El Convenio abarca diversos delitos, como los cometidos a través de la Internet y otras redes informáticas, el fraude informático, la pornografía infantil y las violaciones de la seguridad de las redes, que ya se han incorporado a la legislación nacional de Turquía. Además, el código penal turco abarca el acceso no autorizado a los sistemas de tecnología de la información y la interferencia, interceptación, modificación o destrucción no autorizadas de esos sistemas. Las personas que son condenadas por esos delitos están sujetas a una pena de prisión de hasta tres años o a multas. Posteriormente, se aprobó mediante la Ley de Aprobación de la Ratificación del Convenio sobre la Ciberdelincuencia, y la labor de adaptación en la legislación nacional finalizó en 2016.