Naciones Unidas A/75/123

Asamblea General

Distr. general
23 de junio de 2020
Español
Original: árabe/español/francés/
inglés

Septuagésimo quinto período de sesiones
Tema 98 de la lista preliminar*

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/75/50.

20-08285 (S) 100820 180820

I. Introducción

1. El 12 de diciembre de 2019, la Asamblea General aprobó la resolución 74/28, titulada “Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional”, en relación con el tema 93 del programa, relativo a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

2. En el párrafo 2 de la resolución 74/28, 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 Internacional, a seguir comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

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

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

3. En cumplimiento de esa solicitud, el 27 de enero de 2020 se envió una nota verbal a todos los Estados Miembros para invitarlos a proporcionar información sobre el tema. Como consecuencia de la crisis actual de la enfermedad por coronavirus (COVID-19), a fin de facilitar a los Estados Miembros la presentación de las opiniones sobre las cuestiones antes mencionadas, el plazo original de presentación del 15 de mayo de 2020 se prorrogó hasta el 31 de mayo de 2020.

4. Las respuestas recibidas hasta el momento en que se preparó el informe figuran en las secciones II y III. Las respuestas que se reciban después del 31 de mayo de 2020 se publicarán en el sitio web de la Oficina de Asuntos de Desarme (https://www.un.org/disarmament/ict-security) en el idioma original en que se hayan recibido.

II. Respuestas recibidas de los Gobiernos

Armenia

[Original: inglés]
[13 de mayo de 2020]

Armenia atribuye gran importancia a un ciberespacio abierto, libre, estable y seguro, basado en el pleno cumplimiento de los principios y normas del derecho internacional y de la Carta de las Naciones Unidas, en su totalidad. Teniendo en cuenta el carácter mundial del ciberespacio, es importante proteger los derechos humanos y las libertades en línea, en particular la libertad de opinión y de expresión, que incluye el derecho a buscar, recibir y difundir información. Entretanto, los retos derivados del uso de las tecnologías de la información y las comunicaciones (TIC) y el entorno cibernético son amplios y diversos. Por consiguiente, la comunidad internacional debe permanecer unida en su respuesta para prevenir el uso indebido de las TIC y contribuir a su utilización pacífica y cooperativa. Teniendo esto en cuenta, Armenia participa activamente en plataformas de cooperación internacional para aumentar la transparencia, la previsibilidad y la estabilidad en el ciberespacio y reducir los riesgos de las amenazas derivadas del uso de las TIC.

Armenia está plenamente comprometida con la aplicación cabal del Convenio del Consejo de Europa sobre la Ciberdelincuencia y su Protocolo Adicional relativo

a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Desde 2019, Armenia ha participado activamente en la ejecución del proyecto conjunto de la Unión Europea y el Consejo de Europa CyberEast, cuyo objetivo es aumentar la capacidad en materia de ciberresiliencia, justicia penal y pruebas electrónicas. Del mismo modo, Armenia está aplicando de buena fe las medidas de fomento de la confianza de la Organización para la Seguridad y la Cooperación en Europa (OSCE) (decisión 1202 del Consejo Permanente) para reducir las amenazas derivadas del uso de las TIC. En julio de 2019, Armenia acogió a un equipo de expertos de la División de Amenazas Transnacionales de la OSCE para realizar una evaluación de sus capacidades nacionales en materia de investigación y enjuiciamiento de la ciberdelincuencia. En noviembre de 2019, la División de Amenazas Transnacionales de la OSCE organizó una mesa redonda conjunta en Ereván para examinar las conclusiones de la evaluación mencionada con los interesados armenios. Sobre la base del informe de evaluación de los expertos y las conclusiones de la mesa redonda, la División de Amenazas Transnacionales de la OSCE ha preparado una nota conceptual dedicada al tema, que en el futuro puede convertirse en un proyecto.

El contenido y las conclusiones de los informes de los Grupos de Expertos Gubernamentales de 2013 y 2015 expresan las posiciones de un número limitado de Estados Miembros de las Naciones Unidas que participaron en el proceso de elaboración de los informes de los Grupos de Expertos Gubernamentales, que, por lo tanto, no contribuyeron a la elaboración de un conjunto de normas universales y amplias aceptables para todos los Estados Miembros. En este sentido, creemos que 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, como plataforma inclusiva y transparente para los debates entre los Estados Miembros, puede elaborar una lista consolidada y completa de reglas, normas y principios de comportamiento responsable de los Estados en el uso de las TIC que sea aceptable para todos los Estados Miembros.

Australia

[Original: inglés]
[29 de mayo de 2020]

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

En los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional a partir de 2010 (A/65/201), 2013 (A/68/98) y 2015 (A/70/174) se afirma de manera acumulativa que el derecho internacional vigente, y en particular la Carta de las Naciones Unidas en su totalidad, es aplicable y esencial para mantener la paz y la estabilidad y promover un entorno de tecnología de la información y las comunicaciones abierto, seguro, estable, accesible y pacífico. En los informes también se articulan normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados, reconociendo al mismo tiempo la necesidad de adoptar medidas de fomento de la confianza y de coordinar la creación de capacidad.

Combinadas, estas medidas (derecho internacional, normas, medidas de fomento de la confianza y creación de capacidad) constituyen la base de un ciberespacio seguro, estable y próspero, y a menudo se hace referencia a ellas como un marco para un comportamiento responsable de los Estados.

Australia reafirma su compromiso de actuar de conformidad con los informes acumulativos del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015 (A/65/201; A/68/98; A/70/174). Australia participa activamente en el sexto Grupo de Expertos Gubernamentales y en el Grupo de Trabajo de Composición Abierta inaugural sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (establecido en virtud de las resoluciones 73/266 y 73/27, respectivamente).

Derecho internacional

La posición de Australia sobre la forma en que el derecho internacional rige la conducta de los Estados en el ciberespacio se presenta en la Estrategia de Participación Cibernética Internacional (2017), complementada por el Suplemento de Derecho Internacional de 2019 (ambos disponibles en el sitio web del Departamento de Relaciones Exteriores y Comercio: www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf).

En febrero de 2020, Australia publicó un documento oficioso titulado “Case studies on the application of international law in cyberspace” (estudios monográficos sobre la aplicación del derecho internacional en el ciberespacio) (disponible en los sitios web del Grupo de Trabajo de Composición Abierta: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-studies-final-5-february-2020.pdf; y el Departamento de Relaciones Exteriores y Comercio: www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf).

Aplicación

Recordando que en 2015 la Asamblea General pidió a todos los Estados Miembros “guiarse por el informe de 2015 del Grupo de Expertos Gubernamentales en su uso de las tecnologías de la información y las comunicaciones” (véase la resolución 70/237), Australia ha publicado un panorama general de la forma en que Australia observa y aplica los cuatro pilares fundamentales del informe del Grupo de Expertos Gubernamentales de 2015: el derecho internacional, las normas de comportamiento responsable de los Estados, las medidas de fomento de la confianza y la creación de capacidad (disponible en los sitios web del Grupo de Trabajo de Composición Abierta: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf; y el Departamento de Relaciones Exteriores y Comercio de Australia: https://www.dfat.gov.au/|international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace).

En el informe del Grupo de Expertos Gubernamentales de 2015 se articulan las actividades de mejores prácticas que muchos países estaban o están ya realizando. Australia alienta a todos los países a que hagan un balance de las actividades en curso que se ajusten al informe del Grupo de Expertos Gubernamentales de 2015 (aplicación del derecho internacional, aplicación de normas de comportamiento responsable de los Estados, medidas de fomento de la confianza y creación de capacidad), y a que detecten las lagunas y (si procede) la capacidad necesaria para colmarlas. Junto con México y otros 24 países, Australia se complació en presentar una propuesta al Grupo de Trabajo de Composición Abierta (establecido en virtud de la resolución 73/27) para realizar un estudio de la aplicación nacional de la resolución 70/237 de la Asamblea

General (disponible en los sitios web del Grupo de Trabajo de Composición Abierta: https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf y del Departamento de Relaciones Exteriores y Comercio: www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf).

Género

Como se reconoce en la agenda sobre las mujeres y la paz y la seguridad, las mujeres se ven afectadas de manera diferente y singular por los conflictos y las amenazas a la paz y la seguridad internacionales. Australia encomia el reciente informe del Instituto de las Naciones Unidas de Investigación sobre el Desarme en materia de equilibrio de género en el control de armamentos, la no proliferación y la diplomacia del desarme, titulado “Still behind the curve”, en el que se señala que la Primera Comisión tiene la menor proporción de mujeres diplomáticas de todas las Comisiones Principales de la Asamblea General. La beca Women in International Security and Cyberspace es una iniciativa conjunta de los Gobiernos de Australia, el Reino Unido, el Canadá, los Países Bajos y Nueva Zelandia. Promueve una mayor participación de las mujeres en los debates de las Naciones Unidas sobre cuestiones de seguridad internacional relacionadas con el comportamiento responsable de los Estados en el ciberespacio. Australia seguirá adoptando medidas tangibles para apoyar la participación activa y efectiva de las mujeres en los debates multilaterales relacionados con la seguridad internacional y el desarme.

Bosnia y Herzegovina

[Original: inglés]
[11 de mayo de 2020]

Información sobre las medidas adoptadas a nivel nacional en Bosnia y Herzegovina para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito

El presente informe se basa en los datos reunidos por las siguientes instituciones de Bosnia y Herzegovina: Ministerio de Seguridad de Bosnia y Herzegovina, Ministerio de Defensa de Bosnia y Herzegovina, Ministerio de Transporte y Comunicaciones de Bosnia y Herzegovina, Administración de la Policía Federal, Ministerio del Interior de la República Srpska y Ministerio de Desarrollo Científico y Tecnológico, Educación Superior y Sociedad de la Información de la República Srpska. Las instituciones pertinentes que no habían entregado los datos al Ministerio de Seguridad de Bosnia y Herzegovina antes de que se enviara el informe son: la Policía de Distrito de Brčko y el Ministerio Federal de Transporte y Comunicaciones.

Bosnia y Herzegovina ha firmado acuerdos y convenciones internacionales relativos a la información y la ciberseguridad. Los más destacados son el Convenio sobre la Ciberdelincuencia y el Acuerdo de Estabilización y Asociación. El Convenio se abrió a la firma el 23 de noviembre de 2001 en Budapest, mientras que la Presidencia de Bosnia y Herzegovina adoptó la decisión de ratificar el documento en su 89ª sesión celebrada el 25 de marzo de 2006. De este modo, Bosnia y Herzegovina se vio obligada a aprobar la legislación y otras medidas necesarias para combatir la ciberdelincuencia a fin de armonizarlas con las de otros signatarios del Convenio en lo que respecta al tratamiento de los delitos, la adquisición, el procesamiento y el almacenamiento de datos.

La siguiente legislación es pertinente en Bosnia y Herzegovina en lo que respecta a los temas que abarca la Convención:

- Código Penal de Bosnia y Herzegovina, Boletín Oficial de Bosnia y Herzegovina, 3/03
- Código de Procedimiento Penal, Boletín Oficial de Bosnia y Herzegovina, 3/03, 32/03, 36/03, 26/04,63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09 y 72/13
- Código Penal de la Federación de Bosnia y Herzegovina, Boletín Oficial de la Federación de Bosnia y Herzegovina, 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 y 75/17
- Código de Procedimiento Penal de la Federación de Bosnia y Herzegovina, Boletín Oficial de la Federación de Bosnia y Herzegovina, 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 y 59/14
- Código Penal de la República Srpska, Boletín Oficial de la República Srpska, 64/17 y 104/18
- Código de Procedimiento Penal de la República Srpska, Boletín Oficial de la República Srpska, 53/12, 91/17 y 66/18
- Código Penal del Distrito de Brčko, Boletín Oficial del Distrito de Brčko, 33/13, 26/16, 13/17 y 50/18
- Código de Procedimiento Penal del Distrito de Brčko, Boletín Oficial del Distrito de Brčko, y 33/13, 27/14 3/19

Ámbito estatal

El Ministerio de Seguridad de Bosnia y Herzegovina, motivado por lo anteriormente mencionado y consciente de los riesgos que pueden producirse en el ciberespacio, ha llevado a cabo las siguientes actividades.

A propuesta del Ministerio de Seguridad de Bosnia y Herzegovina, el Consejo de Ministros de Bosnia y Herzegovina, en su 93ª sesión, celebrada el 8 de marzo de 2017, adoptó la Decisión sobre el establecimiento del Equipo Informático de Respuesta de Emergencia para las instituciones de Bosnia y Herzegovina, que se publicó en el Boletín Oficial de Bosnia y Herzegovina, 25/17, estableciendo así el Equipo Informático de Respuesta de Emergencia y ubicándolo en el Departamento de Tecnología de la Información y Sistemas de Telecomunicaciones del Ministerio de Seguridad de Bosnia y Herzegovina.

De conformidad con el artículo 4 de la Decisión mencionada, el Ministerio de Seguridad de Bosnia y Herzegovina debe adaptar su organización interna y la sistematización de los puestos de trabajo a fin de establecer el funcionamiento adecuado del Equipo Informático de Respuesta de Emergencia. A finales de 2017 se recibieron todas las opiniones necesarias de acuerdo con el procedimiento para cambiar la organización interna y la sistematización de una institución, que fueron todas positivas, junto con todos los documentos que se han elaborado.

El Ministerio de Seguridad de Bosnia y Herzegovina ha introducido los cambios y enmiendas necesarios en su organización interna y en la sistematización de los puestos de trabajo a fin de establecer el funcionamiento adecuado del Equipo Informático de Respuesta de Emergencia y los ha entregado al Consejo de Ministros de Bosnia y Herzegovina para su aprobación. Actualmente, se está esperando que el Consejo de Ministros de Bosnia y Herzegovina dé su consentimiento al reglamento propuesto. Una vez recibido el consentimiento, el Ministerio de Seguridad de Bosnia y Herzegovina comenzará a establecer, desde el punto de vista técnico y operacional, el Equipo Informático de Respuesta de Emergencia para las instituciones de Bosnia y Herzegovina. El cambio propuesto en la organización interna incluye cinco puestos

adicionales en la nueva división del Departamento de Tecnología de la Información y Sistemas de Telecomunicaciones.

El Ministerio de Seguridad de Bosnia y Herzegovina tiene previsto reforzar el Equipo Informático de Respuesta de Emergencia desde el punto de vista operacional, institucional y técnico, con el fin de alcanzar los objetivos estratégicos de ese órgano (coordinación y cooperación con los órganos competentes de Bosnia y Herzegovina, eliminación y reducción de las consecuencias de los incidentes de seguridad causados por el acceso no autorizado a los sistemas de tecnología de la información y las comunicaciones (TIC) en las instituciones de Bosnia y Herzegovina, aumento de la fiabilidad de los sistemas de TIC en las instituciones de Bosnia y Herzegovina mediante una dedicación constante, labor de prevención y reducción al mínimo de las posibilidades de que se produzcan incidentes de seguridad y asistencia a los administradores en la aplicación de los incidentes de seguridad, entre otros), realizando actividades de conformidad con el artículo 6 de la Decisión y estableciendo una red de Equipos Informáticos de Respuesta de Emergencia en Bosnia y Herzegovina.

Además, a propuesta del Ministerio de Seguridad de Bosnia y Herzegovina, el Consejo de Ministros de Bosnia y Herzegovina, en su 107ª sesión, celebrada el 6 de julio de 2017, aprobó el análisis sobre la armonización de la legislación en materia de ciberseguridad en Bosnia y Herzegovina y obligó al Ministerio de Seguridad de Bosnia y Herzegovina a intensificar las actividades de elaboración de la estrategia sobre ciberseguridad en Bosnia y Herzegovina.

En consecuencia, se están realizando actividades de armonización de opiniones entre las entidades y los órganos en relación con el modelo del documento estratégico que se sincronizaría con la Directiva de la Unión Europea sobre la seguridad de la información en la red y, por otra parte, cumpliría con la organización constitucional de Bosnia y Herzegovina.

Bajo los auspicios de la Organización para la Seguridad y la Cooperación en Europa (OSCE), se creó un grupo de trabajo oficioso. Este grupo está formado por representantes de instituciones competentes o interesadas de Bosnia y Herzegovina y ha elaborado las Directrices para un marco estratégico de ciberseguridad en Bosnia y Herzegovina.

Además, el Ministerio de Seguridad de Bosnia y Herzegovina participa en las actividades en curso para la elaboración de la nueva estrategia de prevención y lucha contra el terrorismo en Bosnia y Herzegovina, que debería abarcar la utilización del entorno digital para llevar a cabo esas actividades.

El Ministerio de Seguridad de Bosnia y Herzegovina participa activamente en la labor del Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

A propuesta del Ministerio de Seguridad de Bosnia y Herzegovina, el Consejo de Ministros de Bosnia y Herzegovina, en su 80ª sesión, celebrada el 10 de noviembre de 2016, adoptó la Decisión sobre el establecimiento del grupo de trabajo interministerial para la ejecución del proyecto de fomento de la capacidad en materia de ciberdelincuencia (iPROCEEDS) (publicada en el Boletín Oficial de Bosnia y Herzegovina, 14/17).

La Unión Europea y el Consejo de Europa firmaron en enero de 2016 un acuerdo sobre un proyecto regional con el objetivo de crear capacidad en la esfera de la lucha contra la ciberdelincuencia para los países de Europa sudoriental, iPROCEEDS, haciendo hincapié en el decomiso del producto de la delincuencia en línea o de la ciberdelincuencia. La duración del proyecto fue de 42 meses. El proyecto fue financiado por la Unión Europea y el Consejo de Europa, mientras que la ejecución

corre a cargo de la Oficina de Lucha contra la Ciberdelincuencia del Consejo de Europa en Bucarest. Se ha propuesto que el equipo del proyecto que representa a Bosnia y Herzegovina esté compuesto por representantes del Ministerio de Justicia competentes para el delito en cuestión: la fiscalía, la policía y el departamento de inteligencia financiera, entre otros. De conformidad con lo anterior, se ha constituido un grupo de trabajo.

Además, el Ministerio de Seguridad de Bosnia y Herzegovina coordina a los miembros del equipo del proyecto iPROCEEDS-2 sobre la localización del producto del delito en Internet y la obtención de pruebas electrónicas en Europa sudoriental y Turquía, que comenzó en enero de 2020. Este proyecto se basará en los resultados logrados durante la ejecución del proyecto iPROCEEDS y se concentrará en un apoyo específico en las siguientes esferas del proyecto: a) legislación relativa a la seguridad de las pruebas electrónicas y el acceso a los datos, respetando plenamente los derechos y libertades fundamentales, incluida la privacidad y la protección de los datos personales; b) armonización con las normas de protección de datos personales de la Unión Europea y el Consejo de Europa; c) promoción de políticas y estrategias sobre la ciberdelincuencia y la ciberseguridad; d) cooperación interinstitucional y entre los sectores público y privado para la investigación de la ciberdelincuencia y el producto de la delincuencia en línea; e) sistemas de información pública sobre el fraude en línea y otros ciberdelitos; f) capacitación judicial en materia de ciberdelitos y pruebas electrónicas e investigaciones financieras conexas y medidas contra el blanqueo de dinero; y g) cooperación internacional e intercambio de información para la investigación de la ciberdelincuencia y el producto de la delincuencia en línea. La duración del proyecto es de 42 meses.

El Ministerio de Seguridad de Bosnia y Herzegovina desempeña con éxito la función de punto de contacto para la aplicación de las medidas de fomento de la confianza de la OSCE. Algunas de las actividades que se han realizado en este período son la presentación de informes y la entrega de información sobre la situación de la ciberseguridad en Bosnia y Herzegovina, la participación en la labor del grupo de trabajo interministerial reunido en virtud de la decisión 1039 del Consejo Permanente, la participación en siete verificaciones de las comunicaciones y la organización de una capacitación subregional sobre ciberseguridad y seguridad de las TIC en mayo de 2019. También hemos apoyado a la OSCE aportando nuestra capacidad y conocimientos en la organización de varias conferencias y talleres locales.

Además, Bosnia y Herzegovina ha sido incluida en el proyecto regional de creación de capacidad para los profesionales de la justicia penal que luchan contra la ciberdelincuencia y los delitos cibernéticos en Europa sudoriental. El proyecto fue financiado por los Gobiernos de Alemania y los Estados Unidos de América y lo realiza el Departamento de Amenazas Transnacionales de la OSCE en cooperación con representantes de los países de la región (Albania, Bosnia y Herzegovina, Montenegro, Kosovo[1], Serbia y Macedonia del Norte) y las misiones sobre el terreno de la OSCE. El objetivo principal del proyecto es la educación y la capacitación de expertos que trabajan en casos de ciberdelincuencia organizada y delincuencia organizada ciberrelacionada. El proyecto se realizó durante el período 2017-2019 y contribuyó a la elaboración de un marco estratégico general amplio para resolver cuestiones de ciberdelincuencia y amenazas de ciberseguridad, y fortalecer las capacidades existentes para luchar contra la ciberdelincuencia y responder a las amenazas de ciberseguridad. El Ministerio de Seguridad de Bosnia y Herzegovina desempeñó un papel de coordinación para Bosnia y Herzegovina en este proyecto.

[1] Esta designación no afecta a la posición sobre su condición jurídica.

El Ministerio de Defensa de Bosnia y Herzegovina está llevando a cabo actividades con el fin de contar con un sistema de ciberseguridad eficiente y sostenible en su jurisdicción para 2023. Hasta ahora, el Ministerio adoptó la Estrategia de Ciberseguridad para el sector de la defensa el 4 de octubre de 2017. El 27 de diciembre de 2017 se aprobó un plan detallado para la aplicación de esta estrategia. Los objetivos de seguridad se centran en la prevención de los incidentes de seguridad, la respuesta a los incidentes de seguridad, la educación y la certificación del personal que trabaja en la esfera de la ciberseguridad en el sector de la defensa de Bosnia y Herzegovina y el aumento de la conciencia de los usuarios finales en lo que respecta a la seguridad de los sistemas de comunicación e información. Con el fin de aplicar los puntos mencionados, el Ministerio de Defensa de Bosnia y Herzegovina ya ha redactado o aprobado algunos documentos sobre la aplicación.

Además, el Ministerio de Defensa de Bosnia y Herzegovina ha iniciado el proceso de establecimiento de un equipo informático de respuesta de emergencia para el Ministerio de Defensa de Bosnia y Herzegovina.

El Ministerio de Defensa de Bosnia y Herzegovina tiene la obligación, en el marco de la Asociación para la Paz de la Organización del Tratado del Atlántico del Norte, de aplicar el objetivo G7300 de los asociados en materia de ciberdefensa, que requiere: a) la adopción de políticas, procedimientos y otros documentos a fin de lograr una integración visible de la ciberdefensa en las operaciones y procesos de planificación operacional y de que se apliquen reglamentos internacionales en el ciberespacio, medidas de seguridad para el intercambio de riesgos y la estimación de las ciberamenazas entre los órganos nacionales e internacionales en la esfera de la ciberseguridad; b) un Equipo Informático de Respuesta de Emergencia establecido; c) la creación de capacidades para garantizar la confidencialidad, disponibilidad y autenticidad de la información y los sistemas de información del Ministerio de Defensa de Bosnia y Herzegovina y las Fuerzas Armadas de Bosnia y Herzegovina; d) la adopción de programas de educación y capacitación de expertos en la materia y de usuarios finales; e) la adopción de programas educativos mediante la organización de ciberejercicios y seminarios nacionales, así como la participación de representantes del personal del Ministerio de Defensa y de las Fuerzas Armadas de Bosnia y Herzegovina en los ciberejercicios y seminarios internacionales.

A propuesta del Ministerio de Transporte y Comunicaciones de Bosnia y Herzegovina, y en cooperación con el Ministerio de Seguridad de Bosnia y Herzegovina, el Consejo de Ministros de Bosnia y Herzegovina, en su 95ª sesión, celebrada el 22 de marzo de 2017, aprobó la política de gestión de la seguridad de la información para las instituciones de Bosnia y Herzegovina, 2017-2022.

El Ministerio de Transporte y Comunicaciones de Bosnia y Herzegovina trabaja actualmente en la redacción y armonización de una ley sobre la seguridad de la información y la seguridad de las redes y sistemas de información, de conformidad con la Directiva 2016/1148 de la Unión Europea relativa a la seguridad de las redes y los sistemas de información, junto con el Ministerio de Seguridad de Bosnia y Herzegovina. El Ministerio también ha trabajado en un informe sobre la madurez de las capacidades para la estimación de las capacidades en materia de ciberseguridad en Bosnia y Herzegovina, junto con el Centro Global de Capacitación de Seguridad Cibernética de la Universidad de Oxford, el Banco Mundial y el Centro Global para el Desarrollo de la Seguridad Cibernética, entre otros.

En cuanto a las actividades futuras, el Ministerio de Transporte y Comunicaciones de Bosnia y Herzegovina tiene previsto proponer una ley sobre la identificación electrónica en los servicios de confianza para las transacciones electrónicas y elaborar una estrategia para el desarrollo de una sociedad de la información en Bosnia y Herzegovina.

Entidades

Federación de Bosnia y Herzegovina

La Administración de la Policía Federal ha reconocido la importancia de la ciberseguridad y, en consecuencia, en 2015 creó una dependencia de lucha contra la ciberdelincuencia. Esta dependencia y el Centro de Análisis Forense cuentan con el personal, los conocimientos y el equipo adecuados. La dependencia de lucha contra la ciberdelincuencia cuenta con diez expertos, mientras que el Centro de Análisis Forense es miembro de la Red Europea de Institutos de Ciencias Forenses. Esta institución también participa activamente en la ejecución del proyecto de prevención de la explotación y los abusos sexuales de niños en el entorno digital en Bosnia y Herzegovina, junto con el Fondo de las Naciones Unidas para la Infancia, Emaús Internacional y Save the Children. Además, esta institución desempeñó un papel importante en la realización de los proyectos mencionados, como iPROCEEDS y el proyecto de creación de capacidad para los profesionales de la justicia penal que luchan contra la ciberdelincuencia y los delitos cibernéticos en Europa sudoriental, y desempeña también un papel crucial en la ejecución del nuevo proyecto iPROCEEDS-2.

La Federación de Bosnia y Herzegovina adoptó la Decisión sobre la creación del Grupo de Trabajo para la Respuesta de Emergencia Informática para las Instituciones de la Federación de Bosnia y Herzegovina en 2018, con las mismas metas y objetivos que en los dos órganos descritos anteriormente.

República Srpska

El Ministerio del Interior de la República Srpska ha informado de que se han llevado a cabo varias actividades para armonizar la legislación de esta entidad con la de la Unión Europea. Por lo tanto, la República Sprska ha adoptado orientaciones en materia de desarrollo para el período 2017-2021 y un plan de acción para la aplicación de esas orientaciones para el período 2017-2019. Además, ha aprobado un programa de desarrollo de la tecnología de la información y las comunicaciones para el período 2017-2021, que contiene un objetivo centrado en el mejoramiento y la integración del sistema de información y comunicaciones. En consonancia con ello, se ha actualizado la ley sobre la policía y los asuntos internos de la República Srpska y se han creado mecanismos para aplicar el Reglamento 910/2014 de la Unión Europea relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interno y la Directiva 2016/1148 relativa a la seguridad de las redes y sistemas de información.

A propuesta del Ministerio del Interior de la República Srpska, se aprobó la Ley sobre Seguridad de la Infraestructura Crítica (Boletín Oficial de la República Srpska, 58/19), que creó la base para la aplicación de la Directiva 2008/114/CE y la Directiva de la Unión Europea relativa a la seguridad de la información en la red. De este modo, se han creado capacidades legislativas y se ha definido la infraestructura crítica de esta entidad con el fin de reaccionar ante cualquier incidente, incluidos los incidentes relacionados con el ciberespacio.

Además, esta institución participó en el proyecto Instrumento de Ayuda de Preadhesión de 2015, el proyecto para la mejora de la calidad y la seguridad del intercambio de información entre los organismos encargados de hacer cumplir la ley en Bosnia y Herzegovina, el proyecto de creación de capacidad para los profesionales de la justicia penal que luchan contra la ciberdelincuencia y los delitos cibernéticos, el proyecto iPROCEEDS y el proyecto iPROCEEDS-2. Este Ministerio también prepara la infraestructura para el intercambio seguro de datos con otras instituciones y sujetos jurídicos, y presta servicios basados en los mecanismos de seguridad definidos en el Reglamento de la Unión Europea relativo a la identificación

electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Además, se están redactando documentos relacionados con la puesta en marcha de los mecanismos actuales en materia de seguridad de la información.

El Ministerio del Interior de la República Srpska también cuenta con una dependencia especializada para la lucha contra la delincuencia de alta tecnología y, al igual que todos los demás organismos encargados de hacer cumplir la ley en Bosnia y Herzegovina, colabora con la Organización Internacional de Policía Criminal, la Agencia de la Unión Europea para la Cooperación Policial, la Unidad de Cooperación Judicial de la Unión Europea, la Oficina de las Naciones Unidas contra la Droga y el Delito, la OSCE, la Agencia de la Unión Europea para la Formación Policial, la Embajada de los Estados Unidos, el Programa Internacional de Asistencia a la Formación en Investigaciones Criminales, la Asociación Internacional de Policía, el Fondo de las Naciones Unidas para la Infancia y muchas otras embajadas y organizaciones internacionales. La cooperación incluye, entre otras esferas, la educación, la capacitación, los conocimientos y el intercambio de datos.

En lo que respecta a los órganos adicionales para garantizar la ciberseguridad en Bosnia y Herzegovina, la República Srpska aprobó en 2011 la Ley de Seguridad de la Información (Boletín Oficial de la República Srpska, 70/11), que define las normas básicas de seguridad de la información. De conformidad con la Ley, se ha establecido en la República Srpska un departamento para la seguridad de la información, a saber, el Equipo Informático de Respuesta de Emergencia, en el antiguo Organismo para la Sociedad de la Información de la República Srpska (que es ahora el Ministerio de Desarrollo Científico y Tecnológico, Educación Superior y Sociedad de la Información). Este órgano tiene la tarea de coordinar la prevención, la protección contra los incidentes de seguridad informática y la protección de la ciberinfraestructura de los organismos públicos y de las personas jurídicas y físicas. En los dos últimos años, este órgano ha creado el Centro de Operaciones de Seguridad para el gobierno de la República Srpska con el fin de proteger la infraestructura pertinente desde el punto de vista de la seguridad de la información. También se ha llevado a cabo la capacitación de los operadores y se ha comenzado a trabajar en tres turnos. Este órgano trabaja intensamente para recibir la acreditación de las organizaciones internacionales pertinentes o adherirse a ellas.

Canadá

[Original: francés/inglés]
[7 de mayo de 2020]

En el ámbito de la ciberseguridad, el Canadá:

- Se compromete a promover la estabilidad internacional, así como un ciberespacio libre, abierto y seguro
- Considera que el derecho internacional se aplica a la utilización de la tecnología de la información y las comunicaciones por los Estados y refuerza la estabilidad en el ciberespacio
- Alienta a los Estados a que respeten las normas convenidas sobre el comportamiento de los Estados en el ciberespacio, incluidas las normas esbozadas 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, que la Asamblea General hizo suyo
- Considera que las medidas prácticas de fomento de la confianza son un método probado para fortalecer la estabilidad en el ciberespacio

En el plano nacional, el Canadá está actuando de diversas maneras:

- En junio de 2018, el Gobierno, encabezado por el Departamento de Seguridad Pública del Canadá, dio a conocer la Estrategia Nacional de Ciberseguridad del Canadá. La Estrategia tiene por objeto fortalecer las asociaciones para asegurar los cibersistemas vitales, tanto dentro como fuera del Gobierno federal, y proteger a los canadienses y a las empresas del Canadá cuando se conectan en línea. También busca mejorar la detección y la capacidad de respuesta a las ciberamenazas en continua evolución. La Estrategia se organiza de acuerdo con tres objetivos de alto nivel: a) sistemas canadienses seguros y resilientes; b) un ciberecosistema innovador y adaptable; y c) liderazgo, gobernanza y colaboración. El Canadá está aplicando los objetivos de la Estrategia mediante el Plan de Acción Nacional de Ciberseguridad de 2019, en el que se establecen iniciativas concretas durante cinco años.

- Al aplicar la Estrategia Nacional de Ciberseguridad, el Canadá creó el Centro Canadiense de Ciberseguridad, que consolidó las unidades operacionales de ciberseguridad del Gobierno en una organización de cara al público. En su calidad de Equipo Informático de Respuesta de Emergencia del Canadá, el Centro es una fuente unificada de asesoramiento especializado, orientación, servicios y apoyo para el gobierno, los propietarios y operadores de infraestructuras críticas, el sector privado y el público canadiense.

- La Estrategia Nacional de Ciberseguridad de 2018 también incluía la financiación de la nueva Unidad Nacional de Coordinación de la Ciberdelincuencia. Aunque está administrada por la Real Policía Montada del Canadá, la Unidad prestará servicios a todos los organismos policiales canadienses y trabajará con asociados de los sectores público y privado. La Unidad, que estará en pleno funcionamiento en 2023, coordina y armoniza las investigaciones de los ciberdelitos, en diversas jurisdicciones del Canadá y a nivel internacional.

- La Real Policía Montada del Canadá también recibió financiación adicional en 2018 para aumentar la capacidad operacional de inteligencia en materia de investigación y fortalecer los conocimientos técnicos especializados para apoyar las medidas contra las actividades de ciberdelincuencia tanto nacionales como internacionales.

En el plano internacional, el Canadá está actuando de diversas maneras:

- El Canadá participa con la comunidad internacional, los Estados afines y los aliados en múltiples foros internacionales para fortalecer el entorno de ciberseguridad internacional. Por ejemplo, el Canadá sigue promoviendo el desarrollo del derecho internacional y el respeto de las normas convenidas sobre el comportamiento de los Estados en el ciberespacio, incluidas las normas aprobadas por la Asamblea General que se esbozan en el informe del Grupo de Expertos Gubernamentales de 2015. El Canadá también participa activamente en el actual 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 aporta su opinión a los debates del Grupo de Expertos Gubernamentales, según proceda. El Canadá espera que el Grupo de Trabajo de Composición Abierta promueva la aplicación de las normas convenidas y aborde los aspectos de género de la ciberseguridad, entre otras cuestiones.

- En los foros multilaterales de las Naciones Unidas, el Canadá se ha esforzado por promover normas y estándares, y ha instado a los Estados a respetar sus obligaciones en materia de derechos humanos. Ello incluye abordar la violencia contra las mujeres y las niñas facilitada por la tecnología de la información y

las comunicaciones y garantizar su seguridad e integridad personal tanto en contextos en línea como fuera de línea. El Canadá ha tratado de promover esos objetivos de diversas maneras, entre otras cosas, encabezando una resolución en el Consejo de Derechos Humanos sobre la eliminación de la violencia contra las mujeres y las niñas en contextos digitales.

- Guiado por su política de defensa de 2017, “Strong, Secure, Engaged” (protección, seguridad, compromiso), el Canadá se esfuerza por disuadir y responder a las ciberactividades malintencionadas, y aprovecha su cibercapacidad para apoyar las operaciones militares. La cibercapacidad activa de las Fuerzas Armadas del Canadá está sujeta al mismo rigor que otras capacidades militares, incluidas las leyes y obligaciones nacionales e internacionales aplicables y las reglas de enfrentamiento.

- En la Cumbre de Charlevoix de junio de 2018, los líderes del Grupo de los Siete anunciaron la creación del Mecanismo de Respuesta Rápida. El Mecanismo tiene el mandato de coordinar los esfuerzos del Grupo de los Siete para detectar las diversas y cambiantes amenazas a nuestras democracias, incluida la desinformación, y responder a ellas, mediante el intercambio y el análisis de información, y el establecimiento de oportunidades para la respuesta coordinada. El Mecanismo tiene por objeto abordar un amplio espectro de amenazas a la democracia, en beneficio de los miembros del Grupo de los Siete y de la comunidad internacional en general.

Otras iniciativas internacionales en curso son las siguientes:

- Desde 2015, el Canadá ha comprometido más de 4 millones de dólares para apoyar proyectos de creación de capacidad en materia de ciberseguridad. El Canadá también ha financiado la participación de mujeres diplomáticas de América en el Grupo de Trabajo de Composición Abierta, como parte del programa de becas para mujeres en la esfera de la cibernética, que tiene por objeto promover la participación significativa de las mujeres en las cibernegociaciones de las Naciones Unidas.

- El Canadá apoya los esfuerzos de la Organización del Tratado del Atlántico Norte por fortalecer la ciberdefensa de la alianza y de los distintos aliados.

- El Canadá ha estado trabajando en la aplicación de medidas de fomento de la confianza en diversos foros, entre ellos la Organización para la Seguridad y la Cooperación en Europa, la Organización de los Estados Americanos y el Foro Regional de la Asociación de Naciones de Asia Sudoriental.

- El Canadá es miembro activo de Freedom Online Coalition, una organización internacional multilateral que promueve los derechos humanos en línea, en la que preside un equipo de tareas de múltiples interesados sobre inteligencia artificial y derechos humanos.

- El Canadá sigue firmemente decidido a promover los esfuerzos mundiales para garantizar la seguridad y la estabilidad en el ciberespacio, en beneficio de todos.

Colombia

[Original: español]
[29 de mayo de 2020]

En atención a la resolución 74/28 de la Asamblea General, titulada “Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional”, Colombia se permite comunicar al Secretario General, con base en las evaluaciones y recomendaciones que figuran en los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, las siguientes opiniones y observaciones sobre:

- Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional;
- El contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales.

Introducción

Como premisa general, Colombia está a favor de un entorno digital libre, abierto y seguro, garantizando la neutralidad en la red, y en ese sentido considera importante continuar dando prioridad a la creación de capacidades y a la cooperación, sobre la base del derecho internacional y las normas y convenios existentes, así como a la aplicación de medidas de fomento a la confianza en el ciberespacio.

En seguridad digital, Colombia ha realizado esfuerzos importantes en materia cibernética, apostando por una articulación interinstitucional al más alto nivel para garantizar un ciberespacio más seguro.

A partir de la política pública de seguridad digital adoptada en 2016, se creó el Comité de Seguridad Digital, en el que participan las entidades competentes para el tema y que actúa como coordinador ante posibles crisis de seguridad cibernética nacional. El Comité es liderado por un Coordinador Nacional que actualmente es el Consejero Presidencial para Asuntos Económicos y Transformación Digital. La Secretaría Técnica está a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones.

Con esta institucionalidad se busca articular el estudio y la actualización de la política y la normatividad para la seguridad digital y la revisión de la agenda internacional, garantizar la defensa y la seguridad nacionales en el entorno digital, orientando los esfuerzos a mitigar y contrarrestar los ataques cibernéticos, proteger la infraestructura crítica nacional y fortalecer las capacidades humanas, técnicas, tecnológicas y físicas:

- **Grupo de Respuesta a Emergencias Cibernéticas de Colombia.** Instancia del Ministerio de Defensa cuyo propósito es coordinar las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y la defensa nacionales. Es la encargada de responder frente a los incidentes informáticos.
- **Comando Conjunto Cibernético de las Fuerzas Militares.** Ente rector para el direccionamiento, la planeación, la coordinación, la integración, la ejecución y la sincronización de operaciones cibernéticas conjuntas. Su misión es ejercer la ciberdefensa y conducir operaciones militares cibernéticas a nivel estratégico para la seguridad y la defensa de la nación en el ciberespacio, incluyendo la coordinación de las infraestructuras críticas.

- **Centro de Capacidades para la Ciberseguridad de Colombia del Centro Cibernético Policial.** Es la dependencia de la Dirección de Investigación Criminal e Interpol de la Policía Nacional encargada de desarrollar estrategias, programas y proyectos para la seguridad digital, la ciberseguridad y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional, a través de la investigación criminal.
- **Equipo de respuesta a incidentes de seguridad informática.** Colombia cuenta con equipos de respuesta del Gobierno, financiero, sectoriales y privados. A nivel regional, en el marco de la Organización de Estados Americanos, Colombia forma parte de la red hemisférica de equipos de respuesta a incidentes de seguridad informática de las Américas para fortalecer la distribución de alertas en la región.

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 enfrentarlas. Se resalta la importancia del fortalecimiento de la cooperación internacional, entendida no solo como transferencia de conocimientos, tecnologías y mejores prácticas, sino también como acción conjunta y coordinada.

Para los países menos desarrollados tecnológicamente resulta de primordial importancia que se logren entendimientos y 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 o al ser usados como Estados "*proxy*" por la insuficiencia de capacidades para evitarlo.

En estos países, una afectación a determinada infraestructura crítica cibernética puede tener un impacto de grandes proporciones, no solamente por la dependencia de tecnologías de la 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 por la insuficiencia de recursos para fortalecer la seguridad digital de las empresas a cargo de estas infraestructuras.

En consecuencia, se considera que se debe tener en cuenta la ausencia de capacidades como un elemento de riesgo, de lo cual se desprende la necesidad de establecer mecanismos de cooperación internacional para el estudio de riesgos y el fortalecimiento de capacidades.

Igualmente, se estima que la falta de categorización de riesgos y la insuficiencia de medidas de prevención y protección de actividades críticas representan riesgos para los Estados con menor avance en materia de seguridad digital. Asimismo, representa también un riesgo la ausencia de marcos de gobernanza de seguridad digital, lo cual, a su vez, dificulta la articulación interinstitucional e internacional.

Se considera que, más allá de las nuevas amenazas, o de las que puedan surgir posteriormente dado el vertiginoso avance de la tecnología, el tema del comportamiento responsable de los Estados en el ciberespacio, así como de la seguridad de la información y las telecomunicaciones, se debe abordar desde un enfoque trasnacional para que realmente se pueda hacer frente a las amenazas. Se requiere sumar esfuerzos tanto en la difusión oportuna de información, incluido el intercambio responsable de información sobre vulnerabilidades, como en la respuesta efectiva frente a potenciales amenazas.

Colombia reitera su plena disposición para continuar trabajando en la coordinación y el fortalecimiento de la cooperación para estudiar las amenazas actuales y potenciales, así como en las posibles medidas, también de cooperación, para enfrentarlas.

Sobre las normas, reglas y principios voluntarios de comportamiento responsable de los Estados

Colombia coincide plenamente con los conceptos, consideraciones, interpretaciones y recomendaciones consignadas en los informes de los grupos de expertos gubernamentales, en especial el de 2015, que se construyó sobre el trabajo de sus antecesores, y cuyas recomendaciones fueron acogidas ese mismo año por la Asamblea General como guía para el uso de las tecnologías de la información y las telecomunicaciones por parte de sus Estados Miembros.

Las tareas inmediatas deben estar encaminadas a su amplia divulgación y aplicación. No se considera que, por el momento, se requiera un instrumento vinculante en la materia.

Asimismo, resulta importante la cooperación internacional para fortalecer las capacidades nacionales para la implementación de esta normativa.

Colombia, en consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, reitera su disposición para colaborar en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el uso de las tecnologías de la información y las comunicaciones (TIC) y evitar las prácticas en la esfera de las TIC que se consideren perjudiciales o que puedan poner en peligro la paz y la seguridad internacionales.

En ese sentido, el 23 de septiembre de 2019, Colombia apoyó la declaración propuesta por los Estados Unidos sobre el comportamiento responsable de los Estados en el ciberespacio, que comporta un compromiso conjunto de varios países para garantizar una mayor responsabilidad y estabilidad en el ciberespacio a través del trabajo conjunto para ser más efectivos en responder y disuadir actividades cibernéticas maliciosas disruptivas, destructivas y desestabilizadoras. Se resalta que el comportamiento estatal responsable en el ciberespacio debe guiarse por el derecho internacional, la adhesión durante el tiempo de paz a las normas no vinculantes de comportamiento estatal y la implementación de medidas prácticas de fomento de la confianza.

Colombia también apoya el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, iniciativa del Gobierno de Francia, divulgada el 12 de noviembre de 2018, que está a favor de la elaboración de principios comunes para dar mayor seguridad al ciberespacio y que ha recibido el apoyo de varios países, empresas privadas y organizaciones de la sociedad civil.

Igualmente, Colombia apoya el Llamamiento de Christchurch para eliminar los contenidos terroristas y extremistas violentos en línea, una iniciativa de los Gobiernos de Francia y Nueva Zelandia lanzada en mayo de 2019.

Internamente, Colombia cuenta con políticas públicas (que son contenidas en documentos del Consejo Nacional de Política Económica y Social). En 2011, formalizó sus esfuerzos en reconocer a la ciberseguridad y la ciberdefensa como elementos fundamentales para garantizar la defensa nacional. Con ese fin, el Gobierno nacional expidió el documento 3701 del Consejo Nacional de Política Económica y Social, titulado *"*Lineamientos de política para ciberseguridad y ciberdefensa", cuyo objetivo general fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. Se avanzó en tres aspectos fundamentales: a) se establece la institucionalidad en materia cibernética y se imparten lineamientos para ampliar las capacidades del Estado que permitan contrarrestar las amenazas en el ciberespacio; b) se establecen los mecanismos de capacitación en seguridad de la

información y se amplían las líneas; y c) se fortalece la legislación en materia de ciberseguridad.

En 2016 se expidió el documento 3854 del Consejo Nacional de Política Económica y Social, “Política nacional de seguridad digital”, mediante el cual se buscó fortalecer cuatro aspectos fundamentales: a) el marco institucional; b) 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; c) avanzar en la responsabilidad compartida; y d) incluir un enfoque de gestión del riesgo en las actividades que las múltiples partes interesadas realizan en el entorno digital.

A partir de 2019, se está diseñando una política pública de “confianza y seguridad digital”, que contempla dentro de sus objetivos evaluar y actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo. De esta forma se ha propuesto crear un sistema nacional de gestión de incidentes cibernéticos que tendrá como fin: a) articular los esfuerzos institucionales para la gestión oportuna de los incidentes cibernéticos; b) ser la fuente oficial de las estadísticas de los incidentes cibernéticos reportados en el país; c) estandarizar un mecanismo de reporte periódico de incidentes y vulnerabilidades cibernéticas que permita identificarlos, evaluarlos y comunicarlos a los interesados; y d) servir de fuente para la toma de decisiones por parte del Gobierno nacional. Se espera desarrollar la implementación tecnológica del sistema nacional de gestión de incidentes cibernéticos, cuya información podrá ser consultada en tiempo real por los organismos de seguridad del Estado.

Por su parte, en los lineamientos de la política de defensa y seguridad, se establece en los ejes de transformación estratégica la cooperación internacional de Colombia en materia de seguridad, así como la innovación, ciencia y tecnología para el fortalecimiento de las capacidades del sector de la defensa.

En materia de ciberseguridad y ciberdefensa, se hace referencia a la diplomacia en el marco de la seguridad cooperativa a través de la internacionalización del sector mediante alianzas estratégicas, por ejemplo como socio global de la Organización del Tratado del Atlántico Norte en el intercambio de conocimientos, y por medio del programa individual de asociación y cooperación en el fortalecimiento de las capacidades de las fuerzas militares y su articulación conjunta para la atención de amenazas y defensa del ciberespacio.

A su vez, en Colombia se han generado lineamientos basados en las mejores prácticas y estándares internacionales para la creación y funcionamiento de los equipos de respuesta a incidentes de seguridad informática para el sector privado, público y mixtos, para la gestión operativa de los incidentes de ciberseguridad que afectan los intereses nacionales y para impulsar la cooperación, colaboración y asistencia internacional en seguridad digital, ciberseguridad y ciberdefensa con los miembros de los equipos de respuesta de las Américas y de Europa e intercambiar experiencias y buenas prácticas.

Por su parte, el Comando Conjunto Cibernético forma parte del Foro Iberoamericano de Ciberdefensa con el propósito de mejorar la cooperación, compartir lecciones aprendidas, fortalecer las capacidades frente a la gestión de riesgos o amenazas transnacionales en el ciberespacio y participar en ejercicios nacionales e internacionales.

El Centro Cibernético Policial, a través de la operacionalización del Centro de Capacidades para la Ciberseguridad de Colombia, realiza análisis, alertas de prevención y actividades asociadas a la gestión de incidentes de ciberseguridad, así como de la apertura de procesos investigativos en contra del cibercrimen.

Por otro lado, la Comisión de Regulación de Comunicaciones tiene como objetivos: a) generar mecanismos para impulsar la cooperación en materia de seguridad digital entre los prestadores de servicios de comunicaciones y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia; b) centralizar la información sectorial de incidentes de seguridad de la información en la entidad responsable de su gestión; y c) brindar los insumos de información necesaria al Grupo de Respuesta para que realice las actividades de gestión y sensibilización de incidentes en beneficio de las múltiples partes interesadas.

Para el efecto, se expidió la resolución 5569 de 2018 de la Comisión de Regulación de Comunicaciones en la que, entre otras cosas, se estableció que los proveedores de redes y servicios de telecomunicaciones deben implementar un sistema de gestión de seguridad de la información, ajustando sus procesos tendientes a garantizar la integridad, confidencialidad y disponibilidad de los datos.

Es importante resaltar que, para la expedición de la regulación en materia de seguridad digital, se incorporó la recomendación de la Organización para la Cooperación y el Desarrollo Económicos contenida en el documento *Digital Security Risk Management for Economic and Social Prosperity*.

Lo anterior teniendo en cuenta que en la recomendación se plantea que la gestión de riesgos de seguridad digital debe comenzar con la definición de los objetivos económicos y sociales de seguridad o el diseño de las actividades específicas para que, en la etapa de gestión del riesgo, se evalúe cuál es el nivel de riesgo de dicha actividad, determinando todos los resultados posibles sobre los objetivos sociales y económicos.

Posteriormente, en la etapa de tratamiento del riesgo, se determina cómo deberían ser modificadas las estrategias con el fin de aumentar la probabilidad de éxito de la actividad y preservar los objetivos definidos, decidiendo si el riesgo debe ser tomado, reducido, transferido o evitado. Si se decide reducirlo, se pueden seleccionar y aplicar medidas de seguridad o considerar la innovación o las medidas de preparación para su tratamiento.

Así pues, en caso de incidentes relacionados con las TIC, Colombia tiene en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías y la naturaleza y el alcance de las consecuencias.

Específicamente, en lo que respecta a la caracterización de incidentes y su reporte obligatorio a las autoridades competentes, la regulación de la Comisión de Regulación de Comunicaciones también tuvo en cuenta los lineamientos y las buenas prácticas de los estándares 27000 de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) (específicamente las categorías propuestas en el estándar ISO 27035-1) para categorizar los incidentes que se encuentran acotados en la gestión de seguridad de la información. Dicha regulación establece que, cuando se presenten incidentes de seguridad de la información, los proveedores de redes y servicios de comunicaciones deben enviar por medios electrónicos, después de su contención, erradicación o recuperación, un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

En cuanto a la recomendación referida a que “los Estados no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC”, como fue referido en la introducción de este documento, actualmente el Estado colombiano, a través del Comité de Seguridad Digital, del cual forman parte, entre otros, las instancias cibernéticas del Estado, como son el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, el Comando Conjunto Cibernético, el Centro Cibernético Policial y el

equipo de respuesta a incidentes de seguridad informática del Gobierno, se realizan las tareas de prevención y reacción frente a incidentes cibernéticos de cualquier clasificación y tipo en todo el territorio colombiano.

Internacionalmente, Colombia busca cooperar a través del intercambio de información, asistencia mutua e interposición de acciones penales por el uso de las TIC con fines terroristas o delictivos, así como aplicar otras medidas de cooperación para hacer frente a tales amenazas.

En ese sentido, en el nuevo documento del Consejo Nacional de Política Económica y Social de confianza y seguridad digital, que se encuentra en elaboración, se incluye la creación e implementación de un sistema de intercambio de información cibernética con miras a facilitar la divulgación de indicadores de compromiso entre los actores que interactúan en el entorno digital a nivel nacional e internacional. Dicho sistema se articulará con el registro central único de incidentes de seguridad digital.

Por su parte, la Fiscalía General de la Nación utiliza los canales de cooperación internacional de conformidad con los convenios bilaterales y multilaterales establecidos. Sin embargo, se hace necesario la creación de un canal tecnológico seguro o un servicio web para realizar consultas directas y obtener información de los proveedores de servicio de Internet, en su mayoría privados, a fin de que se pueda enviar, recibir, intercambiar y estudiar requerimientos que minimicen el tiempo de respuesta a las solicitudes de asistencia legal mutua.

Los actuales mecanismos presentan el inconveniente de tener un tiempo de respuesta lento, que para efectos procesales es un obstáculo. Es decir, cuando se recibe la contestación, la investigación se encuentra en una etapa en la cual no es viable utilizar dicho resultado dentro del proceso penal.

Asimismo, la Dirección Nacional de Inteligencia ha venido adelantando la coordinación de contactos con agencias homólogas de algunos países a fin de generar un proceso de intercambio de información operacional oportuna, así como la solicitud de ampliación de información referente a casos puntuales que requieren algún tipo de indagación o confirmación.

Esta coordinación aplica para la ampliación de información de casos o tendencias identificadas en el ciberespacio que requieren la correlación de eventos o antecedentes de actividades a fin de poder generar los procesos de seguimiento a estos actores hostiles que llevan a cabo actividades en el ciberespacio.

En relación con la recomendación, los Estados, para garantizar la utilización segura de las TIC, han de acatar las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión. Existen múltiples pronunciamientos de la Corte Constitucional de Colombia sobre el particular.

De la Sentencia de Unificación SU-420 de 2019 se resalta que, en Colombia, la libertad de expresión se aplica en Internet del mismo modo que en otros medios de comunicación, concluyéndose que las redes sociales no pueden garantizar un lugar para la difamación y si bien no es posible supeditar la divulgación de contenido a un permiso o autorización previa, el hecho de que la libertad de expresión goce de cierto carácter prevalente no significa que esta garantía carezca de límites y, por ende, quien ejerce tal derecho está sujeto a las consecuencias que conlleven afectación a terceros.

Por su parte, la Comisión de Regulación de Comunicaciones expidió la resolución 5111 de 2017 “por la cual se establece el Régimen de Protección de los

Derechos de los Usuarios de Servicios de Comunicaciones, se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones", en la que se incorporó el Régimen de Protección a los Usuarios de Servicios de Comunicaciones que estableció que los proveedores de redes y servicios de telecomunicaciones tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes en el interior de sus redes y deben hacer controles periódicos respecto de la efectividad de esos mecanismos. Sin embargo, en caso que un usuario presente una petición, una queja, un reclamo o un recurso que pueda tener relación con un presunto fraude, el proveedor debe investigar sus causas.

Ahora bien, con el fin de identificar las necesidades de asuntos legales, reglamentarios y/o regulatorios que se puedan requerir para promover la seguridad digital y fortalecer las capacidades, en la nueva política de confianza y seguridad digital que se encuentra en elaboración se está incluyendo la realización de un diagnóstico para determinar qué normas podrían requerir ajustes en temas como: a) seguridad de las TIC; b) protección y defensa de la privacidad, libertad de expresión y otros derechos humanos en línea; c) divulgación responsable de vulnerabilidades; d) protección de datos; e) protección al consumidor; f) gestión de riesgos e incidentes; g) centros de respuestas a incidentes, o cualquier otro que se determine; y h) creación de equipos sectoriales de respuesta a incidentes de seguridad informática. Dicho diagnóstico se realizará considerando a las múltiples partes interesadas y deberá determinar la manera en que se adelantarán los ajustes requeridos al marco legal y regulatorio vigente.

Con relación a las recomendaciones relativas a que los Estados deberían tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, en Colombia, adicional a lo ya señalado anteriormente, se busca generar, de forma coordinada con los diferentes actores interesados, el plan de seguridad y defensa de infraestructuras críticas del sector TIC, el cual dicta lineamientos generales para las organizaciones del sector. Este documento es un primer paso para fortalecer y aunar esfuerzos para la protección de la infraestructura crítica identificada.

Internacionalmente, de acuerdo con lo manifestado anteriormente, Colombia coopera y atiende las solicitudes de asistencia de otros Estados para mitigar actividades malintencionadas relacionadas con las TIC. En ese sentido, por ejemplo, el 16 de marzo de 2020 se adhirió al Convenio sobre la Ciberdelincuencia. Asimismo, ha adoptado medidas encaminadas a garantizar la integridad de la cadena de suministro con miras a que los usuarios finales confíen en la seguridad de los productos relacionados con las TIC.

Frente a la divulgación responsable de las vulnerabilidades relacionadas con las TIC y al compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o las infraestructuras dependientes de esas tecnologías, en la nueva política de confianza y seguridad digital que se encuentra en elaboración se contempla el establecimiento de un procedimiento para la promoción y divulgación responsable de vulnerabilidades de los sistemas de información y la infraestructura tecnológica de las entidades del Estado, con el fin de que sean subsanadas por la entidad responsable.

En relación con el funcionamiento de los equipos de respuesta a emergencias cibernéticas o equipos de respuesta a incidentes de seguridad informática, el Gobierno nacional, a través de la política nacional de seguridad digital, establecida mediante el documento 3854 del Consejo Nacional de Política Económica y Social de 2016, dio los lineamientos para la creación de dichos equipos.

Sobre las medidas de fomento de la confianza de carácter voluntario

Para Colombia es de la mayor importancia continuar trabajando en el desarrollo y adopción de medidas de fomento a la confianza y seguridad en el ciberespacio. En el ámbito regional, a través de la Organización de los Estados Americanos (OEA), se ha venido trabajando con este propósito.

En abril de 2017, Canadá, los Estados Unidos, Chile, México y Colombia lideraron la adopción de la resolución sobre el establecimiento de un grupo de trabajo sobre medidas de fomento de cooperación y confianza en el ciberespacio en el Comité Interamericano contra el Terrorismo en el marco de la OEA. En febrero de 2018, Colombia fue elegida para presidir dicho grupo de trabajo. En la segunda reunión del grupo, que tuvo lugar en Chile en abril de 2019, Colombia entregó la presidencia del grupo a Chile.

Las medidas de fomento de la confianza en ciberseguridad, adoptadas en la OEA son:

1. Proporcionar información sobre las políticas nacionales de ciberseguridad, como estrategias nacionales, libros blancos, marcos legales y otros documentos que cada Estado miembro considere relevantes;

2. Identificar un punto de contacto nacional a nivel político para discutir las implicaciones de las amenazas cibernéticas hemisféricas;

3. Designar puntos de contacto, en caso de que no existan actualmente, en los ministerios de relaciones exteriores con el fin de facilitar el trabajo para la cooperación y los diálogos internacionales sobre ciberseguridad y ciberespacio;

4. Desarrollar y fortalecer el desarrollo de capacidades a través de actividades como seminarios, conferencias y talleres sobre ciberdiplomacia, entre otros, para funcionarios públicos y privados;

5. Fomentar la incorporación de temas de ciberseguridad y ciberespacio en cursos de capacitación básica y capacitación para diplomáticos y funcionarios de los ministerios de relaciones exteriores y otras agencias gubernamentales;

6. Fomentar la cooperación y el intercambio de mejores prácticas en ciberdiplomacia, ciberseguridad y ciberespacio mediante el establecimiento de grupos de trabajo, otros mecanismos de diálogo y la firma de acuerdos entre los Estados.

Específicamente, se resalta que las medidas de fomento relativas a los temas de ciberdiplomacia podrían ser un aporte en el que se está trabajando a través de la OEA.

A través de la ciberdiplomacia se pueden buscar caminos para afrontar los desafíos del ciberespacio. Para ello se requiere fortalecer la activa participación de los Estados en los debates internacionales sobre temas de ciberseguridad, lo cual implica la capacitación a los funcionarios diplomáticos en dichas temáticas; pero también incorporar la activa participación de expertos en los escenarios multilaterales.

Por otro lado, se sugiere realizar de forma regular diálogos institucionales con amplia representación, y ampliar y apoyar las prácticas de cooperación entre los equipos de respuesta a emergencias informáticas y los equipos de respuesta a incidentes de seguridad informática.

En relación con la propuesta de establecer una lista global de puntos de contacto, a efectos prácticos se sugiere que se establezca en diferentes niveles, por ejemplo un punto de contacto político/diplomático y otros técnicos (a nivel de policías, fiscalías, equipos informáticos de respuesta de emergencia, etc.).

Será importante determinar quién administraría la información y generar el compromiso de que la misma se mantenga actualizada. Se sugiere contemplar un protocolo de manejo de la información claro y abierto, incluido para el manejo de las bases de datos.

Específicamente en relación con los puntos de contacto nacionales en los niveles técnico y de políticas para abordar los incidentes graves en la esfera de las TIC, para el desarrollo de las temáticas de seguridad digital, el Ministerio de Tecnologías de la Información y las Comunicaciones cuenta con la identificación clara de los responsables de cada temática. Estos datos se pueden compartir con las instancias que lo requieran.

Asimismo, el Ministerio de Tecnologías de la Información y las Comunicaciones cuenta con un directorio de contactos de los directores de tecnologías de la información y de los directores de seguridad de la información de las entidades del Estado, así como de las múltiples partes interesadas, con quienes se han generado espacios de discusión sobre lineamientos de seguridad en el entorno digital y realizado acciones coordinadas en cada una de las fases de la gestión de incidentes por parte de los equipos sectoriales de respuesta a incidentes de seguridad informática del Gobierno.

Sobre el establecimiento de mecanismos y procesos de consulta bilateral, regional, subregional y multilateral, y el dar apoyo a esos mecanismos y procesos, con el objeto de mejorar el fomento de la confianza entre los Estados y reducir el riesgo que representan las percepciones erróneas, la escalada de los incidentes y el conflicto que puedan derivarse de los incidentes relacionados con las TIC, como ya se ha informado, Colombia participa activamente en distintos escenarios internacionales.

Entre ellos, se destaca la participación en los debates llevados a cabo en las Naciones Unidas (en Nueva York, Viena y Ginebra), así como en mecanismos y eventos regionales, principalmente en el marco de la OEA.

En el marco del Grupo de Agenda Digital de la Alianza del Pacífico, con el apoyo de la red hemisférica de equipos de respuesta a incidentes de seguridad informática de las Américas de la OEA, Colombia participa en el proyecto de intercambio de información sobre amenazas cibernéticas entre los Estados miembros de la Alianza del Pacífico. En tal sentido, a partir del 23 de enero de 2020, se encuentra operativa la plataforma tecnológica de intercambio de información entre los equipos de respuesta a incidentes cibernéticos de los países miembros. El nodo nacional de Colombia es operado por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

A nivel bilateral, Colombia suscribió un memorando de entendimiento con Chile sobre ciberespacio, ciberseguridad, ciberdefensa, cibercriminalidad y ciberinteligencia, el cual fue firmado el 21 de marzo de 2019 por los Ministros de Relaciones Exteriores. Las entidades participantes por Colombia son la Consejería Presidencial para los Asuntos Económicos y Transformación Digital, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa, el Centro de Capacidades para la Ciberseguridad de Colombia de la Policía, la Dirección Nacional de Inteligencia, la Fiscalía, el Ministerio de Justicia y la Cancillería.

Con Perú se realizó el intercambio de experiencias en seguridad digital entre expertos gubernamentales de ambos países, llevado a cabo de manera virtual el 15 de abril de 2020. Se intercambió información de las políticas y estrategias nacionales y quedó establecido el canal de comunicación para futuras acciones de apoyo para enfrentar incidentes de seguridad relacionados con las TIC.

Asimismo, Colombia participa en los consejos de innovación en ciberseguridad, una iniciativa de la OEA y Cisco que constituye un escenario para la interacción de los principales líderes de los sectores público y privado, la sociedad civil y el ámbito académico para impulsar la innovación, crear conciencia ciudadana y difundir las mejores prácticas en el campo de la seguridad cibernética en la región. Este espacio es un punto importante en la implementación de las medidas de fomento a la confianza en el ciberespacio y pueden apoyar el avance en la implementación de una política de seguridad digital más efectiva a nivel nacional e internacional.

Cabe señalar que las solicitudes internacionales en materia cibernética generalmente son canalizadas a través de la Coordinación de Prevención del Delito del Ministerio de Relaciones Exteriores.

En relación con la promoción de la cooperación, en particular mediante el establecimiento de centros de coordinación para intercambiar información sobre la utilización malintencionada de las TIC y prestar asistencia en investigaciones, es importante resaltar la labor que se está haciendo por parte de las diferentes autoridades y entidades del Gobierno en la creación de un protocolo nacional de gestión de incidentes, cuyo propósito es lograr una articulación temprana en la atención de incidentes informáticos que puedan atentar contra el orden económico y social o la seguridad nacional. Se resalta la importancia de la aplicación de dicho protocolo dado que busca la identificación del incidente, el estudio del caso, el estudio de la amenaza y la forma de contención o corrección.

Por parte de la Fiscalía General de la Nación, hay tres grupos encargados de temas relativos al ciberdelito, que brindan los apoyos periciales y la asistencia en las investigaciones que provienen de las solicitudes de asistencia legal mutua y en las que se observa la utilización malintencionada de las TIC.

Estos grupos son: a) la Fiscalía Delegada contra la Criminalidad Organizada; b) la Fiscalía Delegada para la Seguridad Ciudadana; y c) la Dirección del Cuerpo Técnico de Investigación. Estos grupos de expertos impulsan dentro de la entidad las nuevas tendencias y buenas prácticas alrededor del ciberdelito y la evidencia digital, aunando a la asistencia en las investigaciones.

Por su parte, la Dirección de Asuntos Internacionales de la Fiscalía se apoya en los diferentes fiscales destacados y en los tres grupos de ciberdelitos de la entidad para impulsar las investigaciones relacionadas con el cibercrimen.

Se resalta el apoyo que ha brindado el Departamento de Justicia de los Estados Unidos, con capacitación en temas relacionados con las solicitudes de asistencia legal mutua. En los Estados Unidos, a las autoridades se les exige cumplir ciertos patrones o estándares de pruebas, con el objeto de lograr acceso a comunicaciones electrónicas almacenadas. En ese sentido, las autoridades requirentes deben presentar hechos articulados cronológicos que demuestren los fundamentos razonables por los cuales consideran que los registros electrónicos son significativos y materiales para una investigación en curso. Se requiere mostrar que existen hechos fundados y fidedignos, no presuntivos, que indiquen que se ha cometido un delito por una(s) persona(s) y que el contenido de la cuenta de correo electrónico o de una red social contiene información del delito objeto de investigación.

De la misma manera, la Dirección Nacional de Inteligencia, de manera bidireccional, realiza coordinaciones de investigación e indagación bajo requerimientos de países que contactan directamente a la organización en el marco de la cooperación internacional.

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

Para Colombia, el tema del fomento de las capacidades es fundamental cuando se hace referencia a asuntos relacionados con la tecnología.

La gestión de riesgos de seguridad digital es un área donde los Estados, el sector privado y la academia pueden trabajar conjuntamente, y en ese sentido se debe pensar en mecanismos de cooperación y asistencia internacional con este fin.

Se resalta la importancia de la participación de las diferentes partes interesadas en el análisis de este tema de la ciberseguridad. Su concurso, tanto en el diagnóstico, como en la adopción de medidas de seguridad preventivas y de respuesta frente a incidentes y emergencias es muy valioso.

Es importante que los Estados internamente empiecen por realizar un diagnóstico sobre las áreas en que requieren fortalecer sus capacidades. Para esto, pueden basarse en los modelos de madurez de capacidades que se han desarrollado internacionalmente.

A partir de ahí, se deben diseñar planes de fortalecimiento que deberían incluir el desarrollo de capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica, diseñados para las instancias y entidades responsables de ciberseguridad, así como de sectores esenciales. Igualmente, y como parte de este fortalecimiento, es importante la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales y sus planes de protección, al igual que los mecanismos de coordinación entre estas.

Dado que este es un asunto que nos compete a todos, es primordial trabajar en la creación de contenidos educativos en materia de seguridad digital, para que sean incluidos en los currículos académicos de los diferentes niveles de formación educativa y cursos no formales.

Frente al establecimiento de procedimientos para la asistencia mutua a la hora de responder a los incidentes y de hacer frente a problemas a corto plazo de seguridad de las redes, incluidos los procedimientos para acelerar la asistencia, Colombia cuenta con un modelo nacional de atención de incidentes, que establece el protocolo de actuación para la gestión de los incidentes que se presenten en todo el territorio nacional, en el cual las instancias cibernéticas actúan según sus competencias y funciones.

Específicamente, el equipo de respuesta a incidentes de seguridad informática del Gobierno fue creado para el fortalecimiento del ecosistema digital en las entidades del Estado, prestándoles servicios de manera gratuita. El catálogo de servicios cuenta con tres frentes enfocados a servicios proactivos, reactivos y gestión de la seguridad. Dentro de los servicios se realiza un monitoreo de disponibilidad de los sitios, se ejecutan análisis de vulnerabilidades, se hace monitoreo de eventos de seguridad, se realiza un acompañamiento en la atención y respuesta a los incidentes y se realiza sensibilización en la atención de incidentes.

El equipo de respuesta a incidentes de seguridad informática del Gobierno se articula con las demás instancias cibernéticas del Estado (Grupo de Respuesta a Emergencias Cibernéticas de Colombia, Comando Conjunto Cibernético y Centro Cibernético Policial) para la gestión de los incidentes de las entidades del Estado y, a través del Comité de Seguridad Digital, participa en la generación de estrategias frente a temas que afectan la seguridad digital de los ciudadanos privados y el Estado.

Con el fin de facilitar la cooperación transfronteriza para hacer frente a las vulnerabilidades de las infraestructuras fundamentales que trascienden las fronteras nacionales, la Fiscalía también articula con los países de la región estrategias de intercambio de información oportuna y ágil en las investigaciones internas en las cuales se tenga conocimiento de la posibilidad de ataques o vulneraciones a infraestructuras fundamentales.

Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones, a través del equipo de respuesta a incidentes de seguridad informática del Gobierno, articula con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia y el Centro Cibernético Policial para validar información a través de las diferentes fuentes internacionales que permitan adelantar acciones de mitigación e investigación cuando estas lo ameriten.

En relación con la elaboración de estrategias de sostenibilidad en las iniciativas de creación de capacidad relativas a la seguridad de las TIC, en los diferentes instrumentos de política pública contenidos en los documentos 3711 y 3854 del Consejo Nacional de Política Económica y Social de 2016 se incluyeron lineamientos y recomendaciones para el fortalecimiento de capacidades. Adicionalmente, se tienen otras medidas administrativas y legales tendientes a fortalecer la capacidad de respuesta, las cuales son emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Ministerio de Defensa, entre otros.

En ese sentido, por ejemplo se han celebrado convenios de cooperación entre el Gobierno de Colombia y la OEA, a través de los cuales las partes aúnan esfuerzos de cooperación técnica con el fin de acompañar la actualización de lineamientos en materia de seguridad digital, y el fortalecimiento de las capacidades y competencias técnicas para la gestión de riesgos cibernéticos mediante iniciativas en dos áreas básicas: a) desarrollo y difusión de políticas; y b) creación de capacidades.

Por su parte, la Fiscalía General de la Nación, a través de la Dirección de Asuntos Internacionales, ha atendido los lineamientos, recomendaciones que los diferentes organismos multilaterales han promulgado para el fortalecimiento de la seguridad en el ciberespacio, con el propósito de realizar una adecuada gestión a las investigaciones de ciberdelitos y de esta manera mitigar en lo posible la impunidad.

La Dirección Nacional de Inteligencia, con la intención de contribuir en las capacidades cibernéticas nacionales, ha decidido crear el equipo de respuesta a incidentes de seguridad informática del sector inteligencia como mecanismo articulador de eventos e incidentes en el sector, y lograr orquestar una dinámica de difusión de información técnica de eventos e incidentes, así como llevar a cabo investigaciones de incidentes cibernéticos.

Igualmente, en Colombia se ha dado prioridad a crear conciencia sobre la seguridad de las TIC, así como a la creación de capacidad en los planes y presupuestos nacionales, con la finalidad de asignar a la seguridad la debida importancia en la planificación del desarrollo y la asistencia. En ese sentido, además de lo ya expresado respecto de las políticas públicas en seguridad digital, se han desarrollado programas de sensibilización sobre la seguridad de las TIC encaminados a educar e informar a las instituciones y los ciudadanos.

En ese sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones se ha esforzado en generar un programa enfocado al desarrollo de capacidades y, a través del establecimiento de acuerdos de cooperación, ha realizado cursos, diplomados y certificaciones en seguridad de la información y gestión de las tecnologías de la información, beneficiando a 1.134 servidores públicos de agencias gubernamentales a nivel nacional y territorial.

Entre ellos se destaca que, en el marco del programa “Hablemos de Gobierno Digital”, más de 250 funcionarios en tecnologías de la información y oficiales de seguridad de entidades públicas participaron en el panel “Construyendo capacidades para el manejo de seguridad y riesgos digitales”.

Se organizó un reto cibernético (“cyberchallenge”) para funcionarios públicos, llevado a cabo en la ciudad de Pereira y en el que participaron 40 líderes de tecnologías de la información. También participaron en un reto de ciberseguridad (“cybersecurity challenge”), donde se enfrentaron a retos, desafíos y situaciones presentes cuando se está en línea. Este ejercicio fue realizado gracias a la OEA con el apoyo de Trend Micro, una firma de ciberseguridad multinacional.

En los talleres “Más Seguridad Digital, Mejor Región”, más de 1.400 funcionarios, entre líderes de tecnologías de la información y oficiales de seguridad de entidades públicas, participaron de forma presencial en los 25 encuentros realizados en 24 ciudades de Colombia.

Con el apoyo de la OEA ha sido posible fortalecer los procesos de capacitación en la región. Por ejemplo, el curso “El Proceso de La Haya: Operaciones de Seguridad Internacional y Ciberespacio”, financiado por el Reino de los Países Bajos, ha sido realizado en varias oportunidades. En 2019 se llevó a cabo en Colombia el curso enunciado en el que, además de la capacitación brindada a funcionarios colombianos, también participaron delegados de América Latina y el Caribe competentes para los asuntos de ciberseguridad. El currículum del curso incluye temas como soberanía, jurisdicción, principio de diligencia, uso de fuerza, derecho internacional de los derechos humanos, ley del mar y acuerdos pacíficos, entre otros temas afines, todo bajo un contexto académico sobre operaciones cibernéticas.

Con relación a la creación de capacidades en técnicas forenses o en medidas de cooperación para hacer frente al uso de las TIC con fines terroristas o delictivos, el Gobierno de Colombia fue anfitrión del “Taller Regional para América Latina sobre Obtención de Evidencia Electrónica de Proveedores de Servicios de Comunicaciones Privados en la Lucha contra el Terrorismo y el Crimen Organizado en Investigaciones Transfronterizas”, organizado por la OEA; la Dirección Ejecutiva del Comité contra el Terrorismo de las Naciones Unidas; la Oficina de las Naciones Unidas contra la Droga y el Delito; la Asociación Internacional de Fiscales; la Coordinación Nacional de Seguridad Digital; y el Ministerio de Tecnologías de la Información y las Comunicaciones. Participaron delegados de 13 países de América Latina (funcionarios pertenecientes a instancias de policía judicial y otras agencias gubernamentales) que se capacitaron en aspectos relacionados con la obtención de la evidencia digital transfronteriza, las actualizaciones legislativas en los Estados Unidos, Canadá y la Unión Europea, las solicitudes de divulgación de emergencia y la redacción de peticiones de asistencia legal mutua, entre otros temas, con el propósito de fortalecer la cooperación internacional en la lucha contra el terrorismo y el crimen organizado.

En los últimos tres años, la Fiscalía General de la Nación ha aprobado la comisión de servicios al exterior de funcionarios de policía judicial adscritos a los grupos de delitos informáticos e informática forense para la asistencia a importantes seminarios y/o capacitaciones organizadas por la OEA y el Registro de Direcciones de Internet para América Latina y Caribe, entre otras, así como con fiscales que conocen y lideran investigaciones relacionadas con la tecnología (como fin o como medio para la comisión de algún delito).

Por otra parte, con el apoyo de entidades privadas y universidades locales, se han impartido varias capacitaciones relacionadas con la lucha contra la cibercriminalidad y la mejora de las técnicas como protocolo y capacitación en

hardware y software de análisis de evidencia digital para poder realizar correlación de casos y detectar patrones.

La Dirección Nacional de Inteligencia, dentro de la articulación del equipo de respuesta a incidentes de seguridad informática del sector inteligencia, planea crear capacidades de pruebas de penetración y análisis de vulnerabilidades, análisis forense y recuperación de información digital, análisis de programas malignos y artefactos cibernéticos, análisis de aplicaciones, laboratorio de fuentes abiertas y estudio de fenómenos cibernéticos.

En atención a la recomendación de elaborar enfoques regionales de creación de capacidades, considerando aspectos específicos de carácter cultural, geográfico, político, económico o social, para propiciar un enfoque adaptado a cada caso concreto, el Ministerio de Tecnologías de la Información y las Comunicaciones, a través del grupo de seguridad y privacidad de la Dirección de Gobierno Digital, viene implementando el Modelo de Seguridad y Privacidad de la Información, que reúne instrumentos que permiten a las entidades del Estado a nivel nacional y territorial hacer frente a amenazas cibernéticas, generando una cultura de seguridad que permita crear conciencia situacional frente a las amenazas cibernéticas que afectan a las organizaciones a nivel transnacional.

Adicionalmente, se viene diseñando entre las autoridades competentes en materia de política criminal un plan nacional que incluye aspectos relacionados con diferentes fenómenos criminales.

La Dirección Nacional de Inteligencia trabaja en la creación de la capacidad de intercambio seguro de información de la Comunidad de Inteligencia Nacional. En ese sentido, se encuentra en proceso de construcción de un proyecto de entrenamiento y generación de capacidades de protección y manejo de buenas prácticas para los países del Caribe en coordinación con la Agencia Presidencial de Cooperación.

En aras de crear capacidad en materia de seguridad en la esfera de las TIC, como ya se ha señalado, Colombia ha participado en iniciativas de cooperación bilateral y multilateral con el fin de mejorar el entorno para prestar asistencia mutua eficaz a la hora de responder a los incidentes relacionados con las TIC.

Así pues, el Ministerio de Tecnologías de la Información y las Comunicaciones viene también desarrollando estrategias de cooperación con empresas de seguridad e instancias cibernéticas a nivel internacional para compartir información de inteligencia de amenazas a nivel estratégico, táctico y operacional.

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

Colombia considera que el derecho internacional aplica a lo “virtual”, al igual que rige para el mundo “físico”, en particular la Carta de las Naciones Unidas e incluyendo el derecho internacional de los derechos humanos y el derecho internacional humanitario.

Coincide con lo manifestado por el entonces Secretario General en el prólogo del Informe del Grupo de Expertos Gubernamentales de 2015, “solo se puede lograr que el ciberespacio sea un entorno estable y seguro mediante la cooperación internacional, y la base de esta cooperación deben ser el derecho internacional y los principios de la Carta de las Naciones Unidas”.

Por ello, Colombia considera que los conceptos generales del derecho internacional pueden tener su aplicabilidad en el ciberespacio, con los ajustes que las operaciones virtuales y sus características requieran.

Considerando las posibles interpretaciones de aspectos asociados al derecho internacional en el ciberespacio, no obsta para que se puedan generar guías o manuales que orienten la aplicación del derecho internacional público al ciberespacio.

En este sentido, la práctica del Convenio sobre la Ciberdelincuencia, que cuenta con notas de orientación con el fin de guiar la aplicación de sus disposiciones y ponerlas en consonancia con los avances en materia de tecnología, podría ser muy beneficiosa. Se estima que es una buena práctica que podría emularse.

Considerando que la Asamblea General de las Naciones Unidas recomendó y acogió el conjunto de reglas, normas y principios internacionales de comportamiento responsable de los Estados, consagrados en los informes de los grupos de expertos gubernamentales, para Colombia la tarea inmediata debe encaminarse a profundizar en dicha normativa y su aplicación. No se considera que, por el momento, se requiera un instrumento vinculante en la materia.

Igualmente, se resalta que Colombia es respetuoso con los compromisos y las garantías adquiridas.

Sobre los conceptos

El desarrollo conceptual que se ha considerado necesario promover para la profundización de los conceptos relativos a la paz y la seguridad internacionales en el uso de las TIC en el plano jurídico, técnico y político, dadas las particularidades y la novedad de su aplicación, deberán continuar siendo discutidas en el marco de los escenarios multilaterales.

Estas discusiones son fundamentales para poder ajustar la normatividad internacional a los desafíos del ciberespacio y generar consensos alrededor de cómo se aplica el derecho internacional en este espacio virtual. En este sentido, Colombia comparte las conclusiones que el Grupo de Expertos Gubernamentales enunció en su informe de 2015 y está presto para ahondar las discusiones con las demás delegaciones en el marco de las Naciones Unidas.

Solo de esta forma se podrá garantizar un uso adecuado de las tecnologías de la información y las comunicaciones, fundamentales para afrontar los desafíos a los cuales se está enfrentando la comunidad internacional en la actualidad, evitando que las mismas sean utilizadas en forma contraria a los objetivos y propósitos de la Carta de las Naciones Unidas, en plena garantía de la paz y la seguridad internacionales.

El uso de nuevas tecnologías para ofrecer servicios de manera disruptiva impulsa una nueva forma de relación en la sociedad de la información, que, al estar basada en el tratamiento seguro de la información y la protección especial de los datos personales, impulsa la promoción de los beneficios de los avances tecnológicos y su aporte al desarrollo social y económico.

Por lo anterior, se considera fundamental robustecer el liderazgo de los Gobiernos para construir una nueva visión de acuerdo con las mejores prácticas internacionales para abordar los riesgos de seguridad digital, teniendo en cuenta principios que apoyen comportamientos responsables por parte de los Estados, que permitan abrir la participación en espacios de discusión en seguridad digital del ámbito internacional y adoptar conductas transparentes y previsibles ante sus pares, reduciendo los riesgos de malinterpretación, escalamiento y conflicto en asuntos de seguridad digital.

Finalmente, la ejecución de estrategias y acciones frente al uso responsable del entorno digital contribuye a la construcción de la paz por medio de la adopción de condiciones apropiadas para lograr la convivencia digital a partir del respeto, apoyando la libertad de expresión y el uso apropiado del lenguaje en la web, pensando en logar aprovechar las ventajas de las TIC y apoyando la adaptación para el futuro digital.

Dinamarca

[Original: inglés]
[29 de mayo de 2020]

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

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

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

El Acuerdo de Defensa para el período 2018-2023 asigna 1.400 millones de coronas danesas al fortalecimiento de la ciberseguridad y la ciberdefensa, reforzando así nuestra capacidad de resiliencia. En la estrategia danesa de seguridad cibernética y de la información de 2018-2021 se adoptaron nuevas medidas para aumentar la ciberseguridad. Mediante 25 iniciativas y 6 estrategias específicas que abordan lo que hasta ahora se ha definido como sectores críticos (energía, finanzas, transporte, atención de la salud, telecomunicaciones y sector marítimo), Dinamarca ha aumentado la resiliencia tecnológica de su infraestructura digital, ha mejorado los conocimientos y aptitudes de los ciudadanos, las empresas y las autoridades, y ha fortalecido la coordinación y la cooperación en materia de ciberseguridad. Además, la Directiva europea sobre la seguridad de las redes y los sistemas de información se ha incorporado plenamente a la legislación danesa.

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

A fin de contar con personal suficientemente capacitado para detectar y manejar los ciberataques contra Dinamarca, en particular en lo que respecta a la infraestructura crítica, el Centro de Ciberseguridad ha desarrollado y puesto en marcha además su propia Ciberacademia intensiva. En 2019 se graduaron en la Ciberacademia 15 personas, que ahora están empleadas en el centro de situación del Centro. Además de la Academia, el Centro de Ciberseguridad también apoya la educación y la investigación en materia de ciberseguridad. Por ejemplo, en 2019, el Centro de Ciberseguridad colaboró con la Escuela de Diseño y Tecnología de Copenhague, la Universidad de Aalborg, la Universidad de Dinamarca Meridional, la Escuela de Negocios de Copenhague y la Universidad Técnica de Dinamarca para llevar a cabo la primera Escuela de Verano sobre Ciberseguridad.

En 2019 se estableció un Consejo de Ciberseguridad público-privado (Cybersikkerhedsråd) para calificar la labor de las autoridades nacionales y el sector privado, fortalecer la democracia digital y mejorar el conocimiento de las amenazas y las oportunidades que traen consigo la digitalización y las nuevas tecnologías.

Con la Estrategia danesa de seguridad cibernética y de la información de 2018-2021, Dinamarca también ha fortalecido su cibercompromiso internacional mediante el envío de ciberagentes a Bruselas; el nombramiento de un cibercoordinador internacional en el Ministerio de Asuntos Exteriores; el nombramiento de un asesor de ciberseguridad en la Oficina del Embajador de Tecnología de Dinamarca en Silicon Valley; y la adhesión al Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte en Tallin. Esto ha permitido a Dinamarca intensificar su participación en ciberforos multinacionales, como los de las Naciones Unidas, la Unión Europea, la Organización del Tratado del Atlántico Norte y la Organización para la Seguridad y la Cooperación en Europa. Dinamarca también es miembro activo del Grupo de Cooperación en materia de Seguridad de la Información en las Redes y de la red del equipo de respuesta a incidentes de seguridad informática y es miembro de la junta de la agencia de la Unión Europea para la ciberseguridad. Mediante su participación en estos foros, Dinamarca ha promovido sistemáticamente un ciberespacio mundial, abierto, estable, pacífico y seguro.

Además, Dinamarca desempeñó un papel activo en el desarrollo de la caja de herramientas 5G de la Unión Europea. La caja de herramientas tiene por objeto establecer un enfoque europeo coordinado de las redes 5G basado en un conjunto de medidas comunes, destinadas a mitigar los principales riesgos de ciberseguridad de las redes 5G.

Dinamarca subraya que, como ha dejado claro la comunidad internacional, el ciberespacio está firmemente arraigado en el derecho internacional vigente, como han atestiguado los Grupos de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional en sus informes aprobados por consenso de 2013 y 2015. El derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplica al comportamiento de los Estados en el ciberespacio. Dinamarca destaca además la importancia de las 11 normas voluntarias y no vinculantes para el comportamiento responsable de los Estados incluidas en los informes del Grupo de Expertos Gubernamentales de 2015, como complemento del derecho internacional vinculante.

A pesar de nuestros esfuerzos conjuntos, la capacidad y la voluntad de los agentes estatales y no estatales de realizar ciberactividades malintencionadas siguen aumentando. Eso debería ser una preocupación mundial. Las actividades malintencionadas en el ciberespacio pueden constituir hechos ilícitos con arreglo al derecho internacional, además de ser desestabilizadoras y entrañar el riesgo de una escalada. Dinamarca sigue decidida a prevenir, disuadir y responder a las actividades malintencionadas y a tratar de mejorar la cooperación internacional a tal efecto. Dinamarca se suma a la Unión Europea para pedir a la comunidad internacional que refuerce la cooperación internacional en favor de un ciberespacio mundial, abierto, estable, pacífico y seguro en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el estado de derecho.

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

Amenazas existentes y nuevas amenazas

Como se ha mencionado, Dinamarca reconoce que el ciberespacio ofrece enormes oportunidades para aumentar el bienestar, impulsar el crecimiento económico sostenible y mejorar la calidad de vida de nuestros ciudadanos. No

obstante, nuestra dependencia de las soluciones digitales también crea ciertos desafíos.

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

Nunca antes la necesidad de un ciberespacio abierto, seguro, estable, accesible y pacífico ha sido tan evidente como durante la pandemia de la enfermedad por coronavirus (COVID-19). Las tecnologías de la información y las comunicaciones (TIC) permiten la comunicación, la colaboración y el intercambio de conocimientos que el mundo necesita para hacer frente a la pandemia.

No obstante, durante la actual crisis de la COVID-19, hemos visto que los agentes malintencionados aprovechan cualquier oportunidad, incluso una pandemia mundial. Esto incluye la interferencia con la infraestructura crítica, como los hospitales que son esenciales para luchar contra la pandemia. Esto es inaceptable y debe ser condenado enérgicamente por todos los Estados. Además, los Estados deben ejercer la debida diligencia y adoptar medidas rápidas y firmes contra la actividad malintencionada de las TIC que tiene origen en sus territorios.

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

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

La comunidad internacional ha dejado claro que el ciberespacio está firmemente arraigado en el derecho internacional vigente, como atestiguan también los Grupos de Expertos Gubernamentales en sus informes aprobados por consenso de 2013 y 2015. Dinamarca pone de relieve que el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplica al comportamiento de los Estados en el ciberespacio.

La soberanía, la no intervención y la prohibición del uso de la fuerza son principios fundamentales del derecho internacional, y su violación por parte de los Estados constituirá un hecho internacionalmente ilícito, para el cual los Estados podrán adoptar contramedidas y pedir reparación en virtud de las normas de responsabilidad del Estado. Todavía hay margen para fortalecer el entendimiento y la interpretación comunes de estos principios fundamentales, y Dinamarca apoya la labor del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional —y otras iniciativas internacionales y regionales— para lograr este resultado.

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

Como se describe en el manual militar de Dinamarca, las operaciones en el ciberespacio no difieren del uso de capacidades militares convencionales en relación con el derecho internacional aplicable. La cuestión también se refleja en la Doctrina

Conjunta para las Operaciones Militares en el Ciberespacio de 2019, en la que se orienta a los dirigentes militares a que incluyan consideraciones sobre el cumplimiento del derecho internacional al realizar operaciones en el ciberespacio. Así pues, el derecho internacional humanitario, incluidos los principios de precaución, humanidad, necesidad militar, proporcionalidad y distinción, se aplica a la conducta de los Estados en el ciberespacio y es totalmente protector, al establecer límites claros para su legalidad, en tiempos de conflicto armado. Dinamarca desea sumarse a la Unión Europea para subrayar que el derecho internacional no es un factor que propicia los conflictos, sino una forma de proteger a los civiles y limitar los efectos desproporcionados.

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

Como ya existe un marco jurídico internacional relativo a las cuestiones cibernéticas, Dinamarca no pide ni ve la necesidad de nuevos instrumentos jurídicos internacionales para las cuestiones relativas al ciberespacio. Sin embargo, hay margen para fortalecer el entendimiento común de cómo se aplica este marco. Dinamarca espera que la labor y las recomendaciones del actual Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta contribuyan a las aclaraciones y faciliten así el tan necesario cumplimiento por parte de los Estados, promoviendo en última instancia una mayor previsibilidad y reduciendo el riesgo de escalada.

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

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

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

Emiratos Árabes Unidos

[Original: árabe]
[31 de mayo de 2020]

Informe nacional sobre las medidas adoptadas por los Emiratos Árabes Unidos para mejorar la seguridad de la información y promover la cooperación internacional en materia de ciberseguridad

Introducción

Los Emiratos Árabes Unidos conceden gran importancia a la ciberseguridad. La protección contra los ataques que utilizan la tecnología de la información y las

comunicaciones (TIC) y que suponen una grave amenaza para la infraestructura, los servicios gubernamentales y las personas es fundamental para mantener la seguridad nacional del país. Por consiguiente, los Emiratos Árabes Unidos se han esforzado por crear un sistema integrado para garantizar la seguridad de los sectores vitales, aumentar la confianza de los usuarios y estimular la innovación.

Medidas adoptadas a nivel nacional para fortalecer la ciberseguridad

El país ha puesto en marcha una estrategia nacional de ciberseguridad, cuyo objetivo es crear un entorno digital seguro y flexible en el que las personas puedan alcanzar sus ambiciones y las empresas puedan crecer. Los objetivos de la estrategia abarcan cinco áreas principales:

1. La aplicación de un marco jurídico y regulatorio amplio para hacer frente a la ciberdelincuencia, proteger las tecnologías actuales y emergentes y permitir que las pequeñas y medianas empresas se protejan contra las ciberamenazas;

2. La elaboración de un programa integrado de sensibilización y creación de capacidad en la esfera de la ciberseguridad, con miras a fomentar prácticas seguras en el uso de la tecnología y desarrollar las aptitudes del personal de ciberseguridad para responder eficazmente a los ataques y asegurar los sistemas y servicios;

3. La elaboración de un plan nacional eficaz que permita una respuesta rápida y coordinada en todo el país a los incidentes de ciberseguridad;

4. La protección de la infraestructura digital de sectores vitales;

5. El fortalecimiento de las asociaciones locales y mundiales de ciberseguridad.

En 2006 los Emiratos Árabes Unidos aprobaron la Ley de Delitos relacionados con la Tecnología de la Información, que contiene numerosas disposiciones que protegen el material privado publicado y difundido en los medios de comunicación basados en las TIC y que castiga el uso indebido de esos medios.

Los Emiratos Árabes Unidos también han puesto en marcha numerosos programas e iniciativas a lo largo de los años para mejorar la ciberseguridad, incluido el Equipo Informático de Respuesta de Emergencia de los Emiratos Árabes Unidos (aeCERT). El equipo presta diversos servicios a los organismos gubernamentales, como la vigilancia e inspección de la infraestructura las 24 horas del día, a fin de detectar y responder directamente a cualquier actividad o ataque inusual; la respuesta efectiva a incidentes de ciberseguridad; y la evaluación de la seguridad de los sitios web y las aplicaciones de telefonía móvil a fin de abordar las vulnerabilidades que pueden explotarse o dar lugar a la fuga de información. El equipo también proporciona a los organismos gubernamentales y a las personas avisos de seguridad e informes periódicos sobre los principales ciberataques, que difunde a través de diversas plataformas, entre ellas, su sitio web, los medios sociales y una lista de distribución.

A fin de garantizar que se apliquen las mejores prácticas de ciberseguridad en todos los sectores vitales del país, se ha creado un sistema de garantía de la seguridad de la información para establecer requisitos de referencia para elevar el nivel mínimo de protección de los activos de seguridad de la información y los sistemas de apoyo.

Junto con las políticas y los sistemas técnicos, era necesario intensificar el desarrollo profesional del personal a fin de aumentar su sensibilización sobre cómo utilizar las TIC de manera constructiva y segura y hacer de ellos la primera línea de defensa contra los peligros de los ciberataques, tanto para su país como para sus familias. Teniendo esto en cuenta, se puso en marcha el programa nacional de

sensibilización y fomento de la capacidad en materia de ciberseguridad para fomentar una cultura de ciberseguridad en la sociedad y la excelencia en las competencias nacionales en materia de ciberseguridad. En el marco de la iniciativa CyberPro, los profesionales de la ciberseguridad asisten a cursos de capacitación de un mes de duración. También se ha creado una academia virtual que ofrece cursos en el mismo campo. Periódicamente se celebran campañas de información pública y eventos dirigidos a distintos segmentos de la sociedad.

El personaje de dibujos animados Salim, creado pensando en la protección en línea de los niños, ha logrado con éxito informar a los niños, de una manera ligera y sencilla, de los principios del uso seguro de la tecnología. Además de un plan de estudios sobre seguridad digital establecido en cooperación con el Ministerio de Educación y la puesta en marcha del sitio web Salim, se han organizado miles de talleres interactivos para educar a los niños mediante cuentos en los que ellos son los protagonistas. Esas iniciativas también han hecho posible que los niños participen en la sensibilización mediante la iniciativa de los embajadores de la ciberseguridad, que les proporciona los instrumentos para difundir la información entre sus pares y fomentar un enfoque seguro y adecuado del tema.

Medidas para fortalecer la cooperación internacional en materia de ciberseguridad

Los Emiratos Árabes Unidos son muy conscientes de que, para lograr un nivel óptimo de ciberseguridad y de capacidad de respuesta a los ataques y riesgos, se requiere cooperación internacional y una actitud seria. Por consiguiente, el país se esfuerza por participar activamente en todos los foros internacionales de ciberseguridad, algunos de los cuales se mencionan a continuación.

El país es miembro de la Unión Internacional de Telecomunicaciones (UIT) y colabora con otros Estados miembros para encontrar soluciones y establecer mejores prácticas de ciberseguridad por conducto de las comisiones de estudio y los grupos de trabajo pertinentes. A los Emiratos Árabes Unidos le complace que algunos de sus propios especialistas ocupen puestos clave en la Unión, como la presidencia del Grupo de Trabajo del Consejo de la UIT sobre Protección de la Infancia en Línea, lo que subraya el compromiso del país de apoyar los esfuerzos mundiales en esas importantes cuestiones.

Los Emiratos Árabes Unidos están representados por el aeCERT en la Junta del Equipo Informático de Respuesta de Emergencia de la Organización de Cooperación Islámica (OIC-CERT), en la que promueve la sensibilización sobre la ciberseguridad mediante la elaboración de programas, manuales y otros materiales esenciales sobre los riesgos en materia de seguridad para las instituciones y las personas. El aeCERT también participa activamente en el Centro de Ciberseguridad de la Región Árabe y en el Comité de Centros Nacionales de Respuesta Informática de Emergencia del Consejo de Cooperación del Golfo (CCG).

Además de colaborar con foros y organizaciones internacionales, los Emiratos Árabes Unidos desean fortalecer la cooperación bilateral en materia de ciberseguridad con países amigos mediante la firma de memorandos de entendimiento y acuerdos para regular el intercambio de información y conocimientos especializados entre los países y la cooperación en respuesta a los ciberataques.

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

Los Emiratos Árabes Unidos desean dar las gracias al Grupo de Expertos Gubernamentales por sus informes sobre los avances en la esfera de la información y

las telecomunicaciones en el contexto de la seguridad internacional. Está de acuerdo con las conclusiones del Grupo sobre la importancia de que los Estados se esfuercen por prevenir las prácticas de TIC perjudiciales, cooperen en la respuesta a los ciberataques, apoyen el diálogo basado en la transparencia y la acción conjunta, respalden el desarrollo mundial de la infraestructura digital y celebren consultas sobre el desarrollo de legislación, estrategias y sistemas de ciberseguridad.

Francia

[Original: francés]
[29 de mayo de 2020]

Francia acoge con beneplácito la oportunidad de responder a la resolución 74/28 de la Asamblea General de las Naciones Unidas, titulada “Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional”, y desea hacer las siguientes aclaraciones.

1. Apreciación general de los problemas 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”.

Francia no considera que la información como tal pueda ser un factor de vulnerabilidad. Además, 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.

Francia considera que el espacio digital debe seguir siendo un espacio de libertad, intercambio y crecimiento que contribuya a la prosperidad y el progreso de nuestras sociedades. 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 malintencionadas que se están desarrollando en el ciberespacio. En efecto, las especificidades del espacio digital (anonimato relativo, bajos costos, fácil acceso a herramientas maliciosas, existencia de vulnerabilidades, proliferación de ciertas herramientas, etc.) permiten a muchos actores desarrollar actividades de espionaje, tráfico ilícito, desestabilización y sabotaje. Si bien algunas amenazas de baja intensidad no guardan relación con la seguridad nacional, sino que constituyen más bien una forma de delincuencia, la utilización de esas herramientas dirigidas contra sistemas informáticos del Estado, infraestructuras de importancia crítica o 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. Francia considera que los Estados deben mantener el monopolio de la violencia legítima, tanto en el ciberespacio como en otros ámbitos. Sin embargo, 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.

2. Esfuerzos de Francia en materia de ciberseguridad en los planos nacional e internacional y opiniones de Francia sobre el contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales

A fin de preservar, desarrollar y promover un ciberespacio abierto, seguro, estable, accesible y pacífico y de hacer frente a las amenazas a la estabilidad y la seguridad internacional, Francia aplica desde hace varios años una política y una diplomacia activas.

La labor de los cinco primeros Grupos de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, en los que Francia participó, permitió avanzar en la definición de principios comunes y en la comprensión colectiva del ciberespacio, en particular en lo que respecta a la cooperación internacional, las normas y la comprensión de la aplicación del derecho internacional.

Actividades de Francia en materia de cooperación internacional, fortalecimiento de la capacidad y promoción y desarrollo de medidas de fomento de la confianza

La acción de Francia en favor de la cooperación internacional en materia de ciberseguridad se desarrolla en un marco bilateral, europeo e internacional.

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 una “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, estabilización y respuesta (sobre todo medidas restrictivas) a los ciberincidentes. Asimismo, participa en el desarrollo de la red CyCLONe, que permite organizar la cooperación operativa entre las agencias nacionales de ciberseguridad europeas en caso de cibercrisis, y en la organización de ejercicios conjuntos para prepararlas, como complemento de la cooperación entre sus centros de vigilancia, alerta y respuesta a los ataques informáticos.

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 OTAN dedique una parte adecuada de sus recursos al fortalecimiento de sus capacidades en materia de ciberdefensa, elevando así el nivel general de seguridad de la Alianza.

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 en ese ámbito. Francia dirige, en particular, junto con otros Estados participantes, la aplicación de una medida de fomento de la confianza en relación con la seguridad de las infraestructuras vitales.

Asimismo, 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 Llamamiento de París, Francia ha subrayado desde 2018 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. 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 para la Confianza y la Seguridad en el Ciberespacio[2] refleja el papel activo desempeñado por Francia en la promoción de un ciberespacio seguro, estable y abierto. El Llamamiento de París, la mayor iniciativa de ciberseguridad de múltiples interesados del mundo, cuenta hasta la fecha con el apoyo de 78 Estados y más de 1.000 entidades no estatales. Su objetivo es 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 ha apoyado también las actividades de la Comisión Mundial sobre la Estabilidad del Ciberespacio, que ha trabajado en la elaboración de propuestas de normas y políticas para fortalecer la seguridad y la estabilidad internacionales y orientar el comportamiento responsable de los Estados en el ciberespacio. El informe que contiene sus conclusiones se presentó en el segundo Foro de París sobre la Paz.

En el marco del Grupo de los Veinte (G20), Francia está trabajando para garantizar que se aborden las cuestiones fundamentales de la competencia en la economía digital y en los nuevos modos de regulación y gobernanza de la seguridad digital, de conformidad con el Llamamiento de París.

Por último, Francia también ha participado en la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Actualmente preside el Grupo de Trabajo de la OCDE sobre la seguridad y la privacidad en la economía digital y tiene previsto trabajar en cuestiones como la responsabilidad de los actores privados, la seguridad de los productos y servicios y la divulgación responsable de las vulnerabilidades.

Por lo que respecta al desarrollo de la capacidad, 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, de manera bilateral o en el marco de iniciativas multilaterales. Además, esa inversión en la cooperación es beneficiosa para todas las partes ya que permite mantener un conocimiento de vanguardia al confrontarnos con nuestros pares y aprender de ellos, enriquecer mutuamente los conocimientos y la experiencia y desarrollar la confianza entre los actores interesados. En los últimos años, Francia también ha desplegado expertos técnicos internacionales en ciberseguridad dentro de las fuerzas de seguridad interior de los países asociados. Por ejemplo, Francia realiza con el Senegal las actividades de la escuela nacional de vocación regional de ciberseguridad de Dakar, que se inauguró a finales de 2018. Este proyecto tiene por objeto proporcionar actividades de formación de corta duración y adaptables para profesionales de la ciberseguridad y altos funcionarios procedentes sobre todo de África Occidental.

La definición de normas de comportamiento responsable, uno de los logros importantes

Francia ha establecido un conjunto de mecanismos, mediante elementos de la doctrina nacional, de gobernanza y de legislación, para aplicar las normas de comportamiento acordadas en los informes del Grupo de Expertos Gubernamentales,

[2] Disponible en https://pariscall.international/fr.

en particular el informe de 2015 (A/70/174). Los siguientes elementos tienen por objeto ilustrar la forma en que Francia ha tratado de aplicar esas normas, pero no pretenden ser exhaustivos.

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

Francia ha adoptado una serie de medidas para cumplir esta norma, en particular consolidando una estrategia nacional de ciberseguridad centrada en la defensa, la prevención, la resiliencia y la cooperación. La revisión estratégica de ciberseguridad, publicada en 2018[3], define una doctrina de gestión de crisis y aclara nuestros objetivos. Confirma el modelo francés que distingue entre las instituciones responsables de las capacidades ofensivas y las que llevan a cabo misiones defensivas. También afirma con firmeza el objetivo diplomático de fomentar la confianza y la estabilidad en el ciberespacio.

Francia también está estableciendo diálogos estratégicos bilaterales sobre cuestiones de ciberseguridad con diversos asociados. Además, participa activamente en muchos foros de cooperación y coordinación regional e internacional, como se ha mencionado anteriormente.

Francia también ha reconocido que tiene capacidad para realizar operaciones militares defensivas y ofensivas en el ciberespacio a fin de garantizar su soberanía nacional, en estricto cumplimiento del derecho nacional e internacional. En un esfuerzo por asegurar la transparencia y la coherencia, ha hecho que sus doctrinas lleguen al mayor número posible de personas mediante la publicación de varios documentos en 2019, en particular elementos de la doctrina militar sobre la guerra informática ofensiva y el libro blanco sobre la aplicación del derecho internacional a las operaciones militares en el ciberespacio. Esta voluntad de aclarar y compartir la visión de Francia debería permitir limitar los malentendidos y las incertidumbres, y contribuir así a consolidar la confianza y la transparencia en el ciberespacio. Francia alienta a todos los Estados a hacer lo mismo.

> Norma b: En el caso de incidentes relacionados con las TIC, los Estados deberían tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías, así como la naturaleza y el alcance de las consecuencias.

Francia ha establecido procedimientos de gestión de crisis, así como estructuras y políticas nacionales en caso de que se produzca un incidente relacionado con la tecnología, en particular:

- Una célula de crisis interministerial, que se desplegará en caso de crisis importante;
- Un centro de coordinación de cibercrisis compuesto de niveles técnicos u operacionales y un nivel estratégico, interministerial y de alto nivel, que se reúne mensualmente. En el caso de un ciberincidente, los participantes del grupo de nivel estratégico lo analizan en un contexto más amplio. Evalúan sus consecuencias y pueden considerar la posibilidad de una atribución. Francia

[3] Disponible www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

considera que la posible atribución de un ataque, así como la decisión de hacerlo público, es una prerrogativa soberana.

Francia ha desarrollado formas de evaluar los incidentes, en particular mediante una escala de gravedad para ayudar a los encargados de adoptar decisiones a analizar y tomar medidas. Para determinar la gravedad de un incidente, Francia tiene en cuenta, por ejemplo, sus consecuencias sobre:

- Los intereses de la nación, su soberanía, la democracia
- La seguridad interna y civil
- La población y el medio ambiente
- La economía

Pueden tenerse en cuenta otros criterios (intencionalidad, peligrosidad, atribución, volumen, recurrencia).

Norma c: Los Estados no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC.

Con el fin de garantizar que su territorio no sea utilizado para actos malintencionados, Francia ha adoptado las siguientes medidas:

- Ha impuesto a los “operadores de importancia vital”, es decir, los operadores de infraestructuras críticas nacionales (ley núm. 2013-1168) y los operadores de servicios esenciales (ley núm. 2018-133) el fortalecimiento de la seguridad de sus sistemas de información y comunicación;
- Ha penalizado (artículo 323-1 del código penal) las intrusiones no autorizadas en los sistemas de seguridad de la información de terceros;
- Ha reforzado la capacidad del Organismo Nacional de Seguridad de los Sistemas de Información para detectar ciberincidentes que afecten a los operadores de infraestructuras críticas (ley núm. 2018-607);
- Ha promovido la divulgación responsable de las vulnerabilidades: las personas que informan a la Agencia Nacional de Seguridad de los Sistemas de Información de la existencia de una vulnerabilidad en un producto o servicio digital están protegidas de posibles acciones legales (ley núm. 2016-1321).

Norma d: Los Estados deberían estudiar cuál es la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines terroristas o delictivos y aplicar otras medidas de cooperación para hacer frente a tales amenazas. Quizás los Estados deberían considerar si existe la necesidad de elaborar nuevas medidas a este respecto.

Además de los elementos mencionados en la sección de cooperación de nuestra respuesta, Francia ha elaborado una serie de medidas para mejorar la cooperación con sus asociados a fin de prevenir la utilización de las tecnologías de la información con fines delictivos y terroristas, en particular mediante su adhesión al Convenio sobre la Ciberdelincuencia (Convenio de Budapest) y al Llamamiento de Christchurch para eliminar los contenidos terroristas y extremistas violentos en línea.

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, por ejemplo, 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 vigilancia, alerta y respuesta a ataques informáticos de todo el mundo.

> Norma e: Los Estados, para garantizar la utilización segura de las TIC, han de acatar las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión.

Francia defiende esencialmente los principios de que los derechos humanos deben respetarse y promoverse en Internet y de que las personas deben poder disfrutar de los mismos derechos en línea que fuera de ella. En el plano nacional, la Comisión Nacional de Informática y Libertades es la autoridad competente encargada, desde 1978, de velar por el respeto de los derechos humanos y las libertades fundamentales, incluido el derecho a la privacidad y la libertad de expresión.

Francia también se ha volcado 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 y las empresas de los Estados Miembros (derecho a la privacidad y a la protección de los datos personales, protección de las infraestructuras críticas, lucha contra los contenidos terroristas en línea). Esta voluntad se reflejó en 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 datos personales y a la libre circulación de esos 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 sistemas de información en 2016, así como en el apoyo a la ampliación de las competencias de la Agencia de la Unión Europea para la Ciberseguridad. 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 de manera independiente. Francia también ha participado activamente en la redacción de las directrices de la Unión Europea sobre la libertad de expresión, aprobadas por el Consejo el 12 de mayo de 2014, para garantizar que la misma libertad de expresión sea efectiva en línea y fuera de línea.

En el Consejo de Europa, Francia apoya las medidas de protección de los derechos humanos en Internet. Por ejemplo, apoyó la adopción de la Guía de los Derechos Humanos para los Usuarios de Internet, preparada por el Comité de Ministros del Consejo de Europa en abril de 2014, en la que se hace hincapié, entre otras cosas, en la libertad de expresión, el acceso a la información, la libertad de asociación, el derecho a la privacidad, la protección de los datos personales y la protección contra la ciberdelincuencia, que deben ser igual en línea y fuera de línea.

En las Naciones Unidas, Francia ha apoyado la adopción de todas las resoluciones del Consejo de Derechos Humanos sobre la promoción de la protección y el disfrute de los derechos humanos en Internet, así como la resolución de la Asamblea General sobre el derecho a la privacidad en la era digital.

En el Foro de París sobre la Paz, celebrado en noviembre de 2018, el Presidente Emmanuel Macron y 11 Jefes de Estado y de Gobierno anunciaron también el

lanzamiento de una iniciativa intergubernamental sobre la información y la democracia, a partir del trabajo ya realizado sobre el tema por la organización no gubernamental Reporteros sin Fronteras. Esta iniciativa se está llevando a cabo en el marco de la Alianza para el Multilateralismo presentada por Francia y Alemania.

> Norma f: Un Estado no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañaran intencionadamente infraestructuras fundamentales que prestan servicios al público o dificultaran de otro modo su utilización y funcionamiento.

De conformidad con esta norma, y como ya se ha mencionado, Francia ha sancionado (artículo 323-1 del código penal) las intrusiones no autorizadas en los sistemas de tratamiento automatizado de datos de terceros.

Además, Francia ha establecido claramente en sus elementos públicos de doctrina, en particular en su libro blanco publicado en 2019 sobre el derecho internacional aplicado a las operaciones en el ciberespacio, la plena aplicación del derecho internacional humanitario a las operaciones cibernéticas realizadas en el contexto de conflictos armados y en relación con ellos, como se examinará con más detalle en la sección sobre el derecho internacional.

> Norma g: Los Estados deberían tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, teniendo en cuenta, la resolución 58/199 de la Asamblea General sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales y otras resoluciones pertinentes.

A fin de contribuir al fortalecimiento de la protección de las infraestructuras críticas, Francia ha elaborado, como se ha indicado anteriormente, un marco reglamentario para la protección de las infraestructuras críticas mediante obligaciones impuestas a los operadores de importancia vital para reforzar la seguridad de los sistemas de información críticos que operan: los sistemas de información de importancia vital (ley núm. 2013-1168, de 18 de diciembre de 2013), así como mediante el fortalecimiento de las competencias de la Agencia Nacional de Seguridad de los Sistemas de Información y su capacidad para detectar incidentes. Los operadores de importancia vital también deben reforzar sus medidas de seguridad y utilizar sistemas de detección aprobados por la Agencia. Francia alienta la cooperación entre el sector público y el privado para desarrollar la protección de las infraestructuras críticas con miras a definir un marco eficaz y apropiado.

> Norma h: Los Estados deberían atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales fueran objeto de actos malintencionados relacionados con las TIC. Los Estados también deberían atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía.

Para aplicar esta norma, Francia ha desarrollado, por ejemplo, una red de cooperación de confianza mediante asociaciones técnicas a nivel de la Agencia Nacional de Seguridad de los Sistemas de Información, que, entre otras cosas, permite los contactos entre centros de vigilancia, alerta y respuesta a los ataques informáticos mediante puntos de contacto permanentes.

Asimismo, Francia ha creado un mecanismo interministerial permanente de análisis de amenazas, preparación y coordinación para la organización de la gestión de crisis en forma de un centro de coordinación de cibercrisis. El centro permite

intercambiar información de manera fluida entre los diferentes servicios con miras a mejorar la coordinación nacional para responder a esas solicitudes.

Francia también ha establecido una red de puntos de contacto en relación con el Convenio de Budapest para permitir la congelación de datos, que está disponible las 24 horas.

En la OSCE, Francia se ha comprometido a poner en práctica la lista de puntos de contacto (medida de fomento de la confianza 8, Decisión núm. 1106 del Consejo Permanente de la OSCE) y a apoyar los diversos esfuerzos para que cada Estado establezca los canales de intercambio y de información adecuados (medida de fomento de la confianza 13, Decisión núm. 1202 del Consejo Permanente).

> Norma i: Los Estados deberían adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro con miras a que los usuarios finales confiaran en la seguridad de los productos relacionados con las TIC. Los Estados deberían tratar de evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC, así como el uso de funciones ocultas y dañinas.

Francia ha fomentado la elaboración de normas y estándares para la industria, en particular mediante el Llamamiento de París. También ha promovido la puesta en marcha de trabajos internacionales sobre el tema en diferentes foros, principalmente a través del Grupo de Trabajo de Economía Digital del G-20 y la OCDE.

Francia ha promovido asimismo la utilización de los principios de certificación de terceros, bajo la autoridad de la Agencia Nacional de Seguridad de los Sistemas de Información, a fin de garantizar el mejor nivel de seguridad que ofrece el mercado. Este proceso está dirigido por el Centro de Certificación Nacional de la Agencia. Francia también ha promovido el establecimiento de ese tipo de certificaciones en la Unión Europea.

Con el fin de reforzar la lucha contra la proliferación de herramientas y técnicas malintencionadas, Francia también ha apoyado la inclusión de los programas informáticos de intrusión en la lista de artículos de doble uso del Acuerdo de Wassenaar.

> Norma j: Los Estados deberían alentar la divulgación responsable de las vulnerabilidades relacionadas con las TIC y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o infraestructuras dependientes de esas tecnologías.

Como se ha indicado anteriormente, Francia ha adoptado diversas medidas para permitir la divulgación responsable de las vulnerabilidades informáticas y ha desarrollado la cooperación a nivel técnico por conducto de la Agencia Nacional de Seguridad de los Sistemas de Información, que intercambia periódicamente información con sus homólogos y asociados sobre las vulnerabilidades y las soluciones disponibles.

> Norma k: Los Estados no deberían realizar ni apoyar de forma deliberada actividades que dañaran los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias cibernéticas o equipos de respuesta a incidentes de seguridad informática) de otro Estado. Un Estado no debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada.

La ley Godfrain (ley núm. 88-19, de 5 de enero de 1988) sobre el fraude informático es la primera ley francesa que castiga los delitos informáticos y la piratería. Penaliza el hecho de acceder o permanecer, de forma fraudulenta, en todo o parte de un sistema de procesamiento automatizado de datos.

El modelo de gobernanza francés, que separa las capacidades ofensivas de las capacidades y misiones defensivas, garantiza el debido respeto de este principio. El Centro Gubernamental de Vigilancia, Alerta y Respuesta a los Ataques Informáticos se dedica principalmente a coordinar e investigar las respuestas a los incidentes cibernéticos para el Gobierno de Francia, pero también para los operadores de infraestructuras críticas y servicios esenciales definidos por la ley, ayudándoles a aplicar el nivel de protección necesario, detectar las vulnerabilidades de las redes y los sistemas, organizar la respuesta a los incidentes con la ayuda de asociados, si es necesario, y participar en una red de confianza de los centros de respuesta a los incidentes de seguridad informática.

El reconocimiento de la aplicación del derecho internacional, incluida la Carta de las Naciones Unidas, al ciberespacio, otro principio acordado en el Grupo de Expertos Gubernamentales

Francia considera que el establecimiento de un marco de ciberseguridad colectiva solo puede basarse en el respeto de las normas existentes del derecho internacional. También 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.

Como concluyó el Grupo de Expertos Gubernamentales en su informe publicado en 2013, los principios y normas del derecho internacional se aplican al comportamiento de los Estados en el ciberespacio. Si bien el ciberespacio presenta características 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.

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 o bajo su jurisdicción, dentro de los límites de las obligaciones que le impone el derecho internacional. La penetración no autorizada de sistemas franceses que tuviera efectos en el territorio francés por medios cibernéticos ofensivos por parte de una entidad estatal o de agentes no estatales que actuaran bajo las instrucciones o el control de un Estado podría constituir una violación de la 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 de los efectos del ataque. Por lo tanto, una operación cibernética puede considerarse un recurso a la fuerza prohibido en virtud del Artículo 2.4 de la Carta de las Naciones Unidas. El cruce del umbral del uso de la fuerza no depende de los medios cibernéticos utilizados, sino de los efectos de la operación. Si estos últimos son similares a los que resultan de las armas clásicas, la operación cibernética puede considerarse 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 las instrucciones de un Estado, cuando alcanza, 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) puede constituir un “ataque armado” en el sentido del Artículo 51 de la Carta de las Naciones Unidas y justificar así la invocación de la legítima defensa.

Esta legítima defensa puede llevarse a cabo por medios convencionales o cibernéticos, respetando 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 a la luz de los criterios establecidos en el derecho internacional.

Además, Francia reconoce la plena 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 se combinan con las operaciones militares convencionales.

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. Este principio también exige que se haga una distinción entre los combatientes o miembros de grupos armados organizados y los civiles. Los ciberataques tampoco deben dirigirse contra la población civil como tal o contra civiles, a menos que esas personas participen directamente en las hostilidades y únicamente durante el tiempo en que lo hagan. En el contexto de un conflicto armado, todo combatiente cibernético de las fuerzas armadas de una parte en el conflicto, 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;

- Los principios de proporcionalidad y precaución. Esas operaciones deben llevarse a cabo velando constantemente por 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 así como su carácter directo (daños al sistema atacado e interrupción del servicio, entre otros) o indirecto (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 pueden ser controladas en el tiempo y el espacio.

Estos elementos se exponen detalladamente en el informe sobre el derecho internacional aplicado a las operaciones en el ciberespacio, publicado por el Ministerio de las Fuerzas Armadas el 9 de septiembre de 2019, y en los elementos públicos de la doctrina militar francesa de la guerra informática de carácter ofensivo presentados ese mismo año.

Por último, Francia considera esencial llegar a un entendimiento común, en el plano internacional, de las obligaciones que incumben a un Estado cuyas infraestructuras se utilizaran con fines malintencionados en contra de los intereses de otro Estado. El objetivo es aclarar la aplicación, en el ámbito cibernético, del principio de la debida diligencia que establece que todo Estado tiene la obligación de "no permitir que su territorio se utilice para actos contrarios a los derechos de otros Estados"[4]. En ese sentido, los Estados no deben permitir a sabiendas que se utilice su territorio para cometer actos internacionalmente ilícitos por medios cibernéticos y deben adoptar todas las medidas que razonablemente se pueda esperar de ellos para garantizar que los agentes no estatales no utilicen su territorio para cometer esos actos. A este respecto, Francia ha identificado el marco de las posibilidades de respuesta a incidentes de los agentes privados como una importante esfera de trabajo, que podría contribuir a limitar las acciones que tienen efectos negativos sobre terceros y, por consiguiente, a respetar el principio de la debida diligencia[5]. Una mejor comprensión de la aplicación de este principio a los desafíos en esta esfera no solo mejoraría la cooperación entre los Estados para proteger ciertas infraestructuras críticas, sino también para detener los ataques cibernéticos de gran envergadura que se realizarían a través de un tercer Estado.

Georgia

[Original: inglés]
[29 de mayo de 2020]

El Gobierno de Georgia, además de promover soluciones de gobierno electrónico seguras, resilientes y fiables y desarrollar la sociedad de la información en general, examina atentamente todas las oportunidades de abordar las recomendaciones del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional sobre la promoción de un comportamiento responsable de los Estados en el ciberespacio. Georgia aspira a contribuir activamente a los principios y directrices del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y a elaborar mecanismos nacionales específicos para ese fin.

En el presente documento se incluyen importantes actualizaciones sobre el desarrollo de la ciberseguridad y la seguridad de la información en Georgia y las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional.

Georgia sigue firmemente decidida a desarrollar su postura de seguridad cibernética y a mejorar de manera comparativa su perfil de ciberseguridad en el ámbito internacional. Las condiciones geopolíticas de Georgia complican sin duda sus esfuerzos de mejorar la ciberseguridad. El 28 de octubre de 2019 se lanzó un ciberataque en gran escala contra los sitios web, los servidores y otros sistemas operativos de la Administración del Presidente de Georgia, los tribunales, diversas asambleas municipales, órganos estatales, organizaciones del sector privado y medios de comunicación. El ciberataque se dirigió contra la seguridad nacional de Georgia con el fin de perjudicar a los ciudadanos y las estructuras gubernamentales de Georgia al perturbar y paralizar el funcionamiento de diversas organizaciones. Gracias a la

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

[5] Este marco —cuyo principio debería informar la labor del Grupo de Expertos Gubernamentales— debería basarse en un análisis de riesgos de las medidas que pueden adoptar los agentes privados en respuesta a un incidente.

investigación realizada por las autoridades de Georgia, junto con la información reunida mediante la cooperación con nuestros asociados, se llegó a la conclusión de que este ciberataque había sido planeado y ejecutado por la División Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia. El incidente mencionado confirma una vez más la importancia de los esfuerzos del Gobierno de Georgia por fortalecer la ciberseguridad a nivel nacional y demuestra de nuevo la necesidad de mejorar la asociación internacional en materia de ciberseguridad.

Georgia dirige todos sus recursos a convertirse en un país más fuerte y seguro en el ciberespacio. En particular, el Gobierno de Georgia se esfuerza por empoderar a todos los grupos destinatarios de la sociedad de la información a fin de que posean el nivel necesario de conocimientos y experiencia para hacer frente a las ciberamenazas. El modelo de gobernanza de Georgia proporciona la capacidad para que las organizaciones públicas y privadas, de forma colectiva e independiente, también puedan garantizar la ciberseguridad del país y la sostenibilidad pertinente mediante el intercambio de recursos. Además, Georgia, en su calidad de interlocutor de confianza en materia de ciberseguridad, goza de la aclamación y el apoyo de sus asociados internacionales.

El Gobierno de Georgia se esfuerza activamente por proporcionar un ciberespacio abierto y seguro. La ciberseguridad es una dirección estratégica de la política de seguridad nacional del Gobierno de Georgia, y se presta una gran atención política a hacerla más avanzada y resiliente. El Gobierno considera que su prerrogativa es establecer un entorno propicio para la sociedad de la información, la economía digital y el gobierno electrónico en el país; el Gobierno asume la responsabilidad de crear marcos estratégicos institucional-organizativos y jurídico-reguladores pertinentes que apoyen la realización de funciones seguras en un entorno electrónico por parte de los ciudadanos y los sectores público y privado, siempre que utilicen el espacio en línea de manera segura.

El fortalecimiento de la cooperación bilateral, regional e internacional en la esfera de la ciberseguridad ha ocupado un lugar destacado en el programa político del Gobierno de Georgia. Georgia constituye un buen ejemplo de asociación en los planos regional e internacional, y en formatos multilaterales (Unión Europea, Organización del Tratado del Atlántico del Norte (OTAN), Organización para la Seguridad y la Cooperación en Europa (OSCE), Naciones Unidas, Asociación Oriental, Consejo de Europa, Agencia de la Unión Europea para la Cooperación Policial, Organización Internacional de Policía Criminal, Agencia de la Unión Europea para la Formación Policial, Agencia de la Unión Europea para la Ciberseguridad). Georgia participa activamente en proyectos y reuniones internacionales relacionados con la ciberseguridad.

En los últimos años se han llevado a cabo las siguientes iniciativas de cooperación y asociación:

- Las medidas destinadas a fortalecer la ciberseguridad que ha adoptado Georgia en el último decenio son positivas, y las reformas aplicadas y los procesos en curso se evalúan positivamente a nivel internacional. Georgia ocupa un lugar destacado y una posición de liderazgo en cuanto al desarrollo de la ciberseguridad entre los países de la Asociación Oriental, razón por la cual el país desempeña la función de centro regional de ciberseguridad en las múltiples actividades de creación de capacidad e intercambio de información y mejores prácticas de los países de la región.
- La cooperación entre Georgia y la OTAN en materia de ciberseguridad está en fase de desarrollo. Georgia se encuentra en una etapa activa de colaboración con los Estados miembros de la OTAN y participa tanto individual como

colectivamente en diversos proyectos administrados bajo el patrocinio de la OTAN. Esto incluye también la participación de Georgia en iniciativas de aprendizaje estratégico o técnico. La OTAN (sede y oficina de enlace) ayuda a las ciberautoridades de Georgia a realizar actividades sistemáticas y continuas de sensibilización y capacitación en toda Georgia dirigidas a diferentes grupos de destinatarios. Georgia presenta regularmente sus logros e iniciativas en materia de ciberseguridad a la Comisión OTAN-Georgia y se guía de cerca por el compromiso de la OTAN en materia de ciberdefensa.

- Georgia y la Unión Europea. Mediante el programa quinquenal de la Unión Europea para la seguridad, la rendición de cuentas y la lucha contra la delincuencia en Georgia "EU4 Security, Accountability and the Fight against Crime in Georgia", el país recibe asistencia de la Unión Europea en las esferas de la ciberdelincuencia, la gestión de las amenazas cibernéticas e híbridas, la gestión de las fronteras, la protección civil y la supervisión del sector de la seguridad. Georgia fortaleció su cooperación en el marco de la plataforma de la Política Común de Seguridad y Defensa de la Unión Europea, que se hace eco de los objetivos estratégicos de la organización definidos internacionalmente y, en su conjunto, al desarrollar la capacidad de defensa de Georgia, apoya la consolidación de su seguridad nacional.

- Georgia y la OSCE. Georgia considera de gran valor la creación de una red de confianza entre los países asociados, facilitada por las medidas de fomento de la confianza en el ámbito de la ciberseguridad. Los puntos de contacto de Georgia participan activamente en la plataforma de ciberseguridad de la OSCE y sus iniciativas.

- Los Gobiernos de Georgia y el Reino Unido firmaron el Memorando de Entendimiento sobre cooperación en materia de ciberseguridad. Su objetivo es mejorar el trabajo mutuo, compartir las mejores prácticas y alinear mejor los enfoques sobre los diferentes aspectos de la ciberseguridad.

- Georgia y los países de la Asociación Oriental. El Organismo de Intercambio de Datos sigue cooperando con los países de la Asociación Oriental en el marco del programa de la Unión Europea para la mejora de la ciberresiliencia en los países de la Asociación Oriental "EU4 Digital: Improving Cyber Resilience in the Eastern Partnership Countries". El proyecto CyberEast ayuda a Georgia y a otros países de la Asociación Oriental a aumentar las capacidades de ciberresiliencia, justicia penal y pruebas electrónicas de los países de la Asociación Oriental, para luchar mejor contra la ciberdelincuencia. La atención se centra en mejorar los marcos jurídicos y normativos; reforzar la capacidad de las autoridades judiciales y de las fuerzas del orden y la cooperación interinstitucional; e introducir mecanismos eficientes de cooperación internacional para aumentar la confianza en la justicia penal, la lucha contra la ciberdelincuencia y las pruebas electrónicas, incluso entre los proveedores de servicios y los encargados de hacer cumplir la ley.

- Georgia sigue fortaleciendo la cooperación regional con los países vecinos en el marco de la Organización para la Democracia y el Desarrollo Económico. En 2019, los representantes de Georgia participaron en reuniones en los locales de la Organización para la Democracia y el Desarrollo Económico en Kiev.

- El Equipo Informático de Respuesta de Emergencia, una dependencia subsidiaria del Organismo de Intercambio de Datos del Ministerio de Justicia de Georgia, ha firmado un número considerable de memorandos de cooperación para compartir conocimientos y experiencia con las respectivas organizaciones de los países de Europa y la Asociación Oriental (Lituania, Rumania, Moldova,

Ucrania y Belarús). Georgia participa activamente en los ciberejercicios y programas de estudio internacionales, en los que el país ocupa constantemente los primeros lugares en cuanto a resultados observados.

En la práctica, Georgia, con sus amplios conocimientos nacionales en la materia, considera que los mejores y más pertinentes conocimientos especializados internacionales constituyen una valiosa orientación y oportunidades de cooperación para el desarrollo de sus pilares estratégicos, jurídicos, institucionales y de creación de capacidad, así como para el proceso de transformación de la cibercultura.

Con la cooperación activa de los organismos sectoriales en el ámbito de la ciberseguridad[6], en 2019 se elaboró en Georgia el tercer proyecto de estrategia nacional de ciberseguridad y su plan de acción[7]. La Oficina del Consejo de Seguridad Nacional desempeñó un papel de coordinación en este proceso. Al mismo tiempo, los interesados pertinentes del sector privado, los círculos académicos y la sociedad civil también participaron en las actividades respectivas. A medida que Georgia se esfuerza por armonizar su marco nacional con los respectivos mecanismos euroatlánticos, el proceso de desarrollo estratégico está fuertemente asesorado por expertos extranjeros y consultores nacionales en la materia. De especial importancia en el contexto de la elaboración de la estrategia nacional de ciberseguridad y su plan de acción fue la asistencia prestada por el Reino Unido a los agentes de ciberseguridad de Georgia pertinentes. El proyecto de estrategia nacional de ciberseguridad y su plan de acción serán aprobados por el Gobierno de Georgia durante 2020. Los documentos respectivos se someterán al examen de la comisión interinstitucional permanente creada en enero de 2020 en el Consejo de Seguridad Nacional y a la que se ha confiado la función de coordinar la elaboración de los documentos conceptuales de ámbito nacional en materia de seguridad. Posteriormente, el Consejo de Seguridad Nacional presentará los proyectos de documentos al Gobierno de Georgia para su aprobación.

Georgia sigue reforzando la aplicación de los marcos jurídicos y regulatorios en el ámbito cibernético. Se han aplicado amplios marcos legislativos y regulatorios en el ámbito de la tecnología de la información y las comunicaciones que abordan la ciberseguridad, y Georgia ha aprobado legislación que protege los derechos de las personas y las organizaciones en el entorno digital. Las leyes abordan la protección de la infraestructura de información crítica, la responsabilidad de los proveedores de servicios de Internet, la obligación de notificar incidentes y la seguridad de las transacciones electrónicas. Como siguiente paso, Georgia tiene planes ambiciosos para armonizar su marco jurídico de ciberseguridad con la Directiva de la Unión Europea sobre la seguridad de las redes y sistemas de información. Los organismos responsables iniciaron en 2019 el proceso de cooperación con la Unión Europea y, para finales de este año, se elaborará una ficha de hermanamiento, con el fin de ayudar a Georgia en el proceso de armonización. Como resultado del proyecto de hermanamiento, Georgia actualizará su Ley de Seguridad de la Información, en la que, entre otros aspectos importantes, se definirá claramente un marco de gobernanza de ciberseguridad, las autoridades para la Directiva y las funciones y responsabilidades en materia de ciberseguridad en los planos estratégico, operacional y táctico.

Georgia también ha iniciado otro ambicioso proceso de diseño y adopción de un modelo compatible con la Unión Europea para la protección de la infraestructura de información crítica. Durante 2019 se celebraron varios talleres con el fin de examinar un sistema adecuado de identificación y cooperación con infraestructuras críticas en el ámbito cibernético. Georgia creó una metodología y cuestionarios pertinentes para

[6] Agencia de Intercambio de Datos (Ministerio de Justicia), Oficina de Ciberseguridad (Ministerio de Defensa), Agencia Operativa-Técnica (Servicio de Seguridad del Estado).

[7] Previsto para el trienio 2020-2023.

las infraestructuras de información críticas. El proceso incluyó debates con representantes de sectores críticos de propiedad privada de diferentes ámbitos sectoriales y empresariales.

Actualmente, la política de seguridad de la información y los requisitos de ciberseguridad están en proceso de aplicación en todas las organizaciones definidas como infraestructuras de información críticas. Los organismos estatales responsables ayudan a estas entidades a aplicar las políticas de seguridad de la información y los elementos esenciales de la ciberseguridad, proporcionando recomendaciones, conocimientos especializados y capacitación, así como mediante actividades más amplias, como auditorías de seguridad de la información, pruebas de penetración y otros servicios de información y ciberseguridad. Se han puesto en marcha varios proyectos para la aplicación de un sistema de gestión de la seguridad de la información en los organismos que forman parte del sistema de información crítica. Estas entidades reciben apoyo para la adopción de políticas de seguridad de la información, tareas de gestión de activos y exámenes de políticas. Al mismo tiempo, el Gobierno establece normas y procedimientos para la seguridad de la información mediante leyes y reglamentos (basados en la familia de normas ISO 27000) e imparte cursos de capacitación sobre seguridad de la información para representantes del Gobierno y del sector privado. El siguiente objetivo es elaborar y aprobar disposiciones jurídicas sobre la protección de la infraestructura de información crítica armonizadas con la Directiva de la Unión Europea sobre la seguridad de las redes y sistemas de información, garantizando que las disposiciones jurídicas ampliadas relativas a la seguridad de las redes y sistemas de información sean aplicables a la protección de la infraestructura de información crítica.

El Gobierno de Georgia utiliza con éxito las plataformas de múltiples interesados de los sectores público y privado como instrumento para crear confianza entre todos los interesados y compartir información y conocimientos, poner en marcha nuevas iniciativas y permitir la participación del sector privado en el proceso de elaboración de políticas y estrategias. El Organismo de Intercambio de Datos, que dirige el proceso de cooperación entre los sectores público y privado, organizó numerosos talleres y reuniones durante 2019 con los sectores financiero, energético y de las telecomunicaciones, a fin de unirse a las consultas preparatorias del proceso de identificación de la infraestructura crítica. Las partes interesadas del sector privado participan en todos los principales procesos de consulta sobre proyectos horizontales en iniciativas estratégicas, políticas, jurídicas, regulatorias y de fomento de la capacidad.

Georgia lleva a cabo actividades sistemáticas y continuas de sensibilización y capacitación para fomentar el ciberprofesionalismo y la competencia, dirigidas a diferentes grupos destinatarios. Gracias a la participación de las organizaciones estatales de Georgia, se han llevado a cabo campañas de sensibilización en gran escala destinadas a aumentar el nivel de conocimientos de la población sobre la ciberhigiene; asimismo, en la actualidad, se están organizando activamente programas de aprendizaje y readiestramiento profesional para diversos grupos destinatarios en el ámbito de la ciberseguridad. Año tras año, el nivel de madurez de la capacidad de Georgia en materia de ciberseguridad mejora como resultado de diferentes iniciativas y programas educativos. El Gobierno ha sido y es muy activo en sus intentos por elevar la cualificación de los profesionales de la ciberseguridad que trabajan en el sector público. En consecuencia, su competencia profesional es elevada y muchos de ellos poseen certificados internacionalmente reconocidos y de gran reputación (Instituto SANS, Asociación de Auditoría y Control de los Sistemas de Información, Organización Internacional de Normalización).

Por último, Georgia seguirá participando activamente en el diálogo internacional sobre la gobernanza de Internet y otras iniciativas internacionales relacionadas con la ciberseguridad colectiva.

Honduras

[Original: español]
[17 de abril de 2020]

Informe sobre las medidas adoptadas en materia de ciberespacio en el contexto de la seguridad internacional

En el marco de la norma de la Organización Internacional de Normalización (ISO) 27001 (norma internacional de seguridad de la información), y con el propósito de crear una cultura laboral en armonía con la iniciativa del gobierno digital impulsado desde la presidencia de la República, la Policía Nacional de Honduras realiza diferentes esfuerzos internos, centrándose en el uso responsable de los recursos de Internet apegados al "Manual de Seguridad de la Información" de la institución policial, donde se expresa claramente la política establecida para resguardar los diferentes aspectos que aseguran las actividades operativas de nuestros funcionarios y disminuyen la brecha de vulnerabilidades de ser víctimas de cualquier ataque o acción malintencionada contra nuestros sistemas.

Algunas de las medidas adoptadas en materia de ciberespacio por la Policía Nacional son:

1. Elaboración de la política de seguridad de la información

Establece las normas y directrices para el uso adecuado de las herramientas tecnológicas, buscando proteger los recursos informáticos y físicos de la institución como insumo fundamental para el cumplimiento de la misión constitucional y asegurar el mejoramiento continuo, administrándola y protegiéndola a través de la aplicación efectiva de las mejores prácticas y controles, garantizando la confidencialidad, disponibilidad e integridad de la información en general.

2. Jornadas de capacitación

La Policía Nacional de Honduras, a través de la Dirección Policial de Telemática, realiza permanentemente jornadas de concientización en materia de ciberespacio dirigidas al personal operativo y administrativo, y participa en actividades extraordinarias realizando capacitaciones en temas como el ciberacoso, la ingeniería social, las noticias falsas, el cibercrimen y la ciberseguridad.

3. Implementación de una red local

Mediante la página de nuestra Intranet llamada "Poliweb" se mantiene informado a nuestro personal sobre las últimas tendencias en ciberdelitos y se dan a conocer boletines informativos de alta importancia sobre acontecimientos reales de nuestro entorno relacionados con la ciberseguridad y la difusión de políticas emanadas del manual de seguridad de la información para la conservación de la seguridad informática.

Esta modalidad de conectividad interna permite que todas las operaciones dentro de la Policía Nacional se realicen a través de nuestra red local o Intranet, de manera que se minimiza el riesgo de que nuestros usuarios ingresen a sitios desconocidos, lo cual genera también un ahorro en el consumo de los recursos de Internet y ancho de banda.

4. Control e investigación de incidentes

El equipo de seguridad de la información mantiene el monitoreo permanente de la red de datos institucional, identificando las vulnerabilidades y amenazas que nuestros usuarios puedan llegar a permitir en sus equipos, ya sea por navegación inadecuada o intento de saltos a nuestras restricciones; simultáneamente se desarrollan acciones para la investigación y el control de incidentes informáticos en la red institucional. Las Secciones de Administración de la Información y Control de Incidentes del Departamento de Seguridad de la Información analizan las vulnerabilidades conocidas que podrían poner en riesgo los sistemas de la institución y su información. Por tanto, estas son adecuadamente gestionadas y remediadas, para lo cual se implementará un procedimiento formal, que contempla:

- Adicionar a los inventarios de activos de información los datos correspondientes al proveedor del *software*, versión, estado actual de despliegue y funcionario responsable del *software*;
- Realizar análisis de vulnerabilidades semestralmente;
- Mantener información actualizada de nuevas vulnerabilidades;
- Definir la línea de tiempo para aplicar las correcciones y soluciones para las vulnerabilidades conocidas;
- Probar las correcciones o parches de remediación de vulnerabilidades antes de su despliegue en los ambientes de producción.

5. Auditorías

Mediante la ejecución del plan anual de auditorías se verifica el cumplimiento de las políticas emanadas para el correcto uso de los equipos informáticos, así como del Internet institucional.

Algunas de las restricciones establecidas son:

- Prohibir la instalación de redes privadas virtuales (VPN) en las computadoras;
- Prohibir navegadores diferentes incógnitos como TOR, i2p, DUCK y WHONIX;
- Prohibir el uso de redes sociales (con excepciones para direcciones especiales);
- Prohibir la navegación en sitios de alto consumo de transmisión en línea como la televisión digital o de reproducción de video;
- Prohibir el almacenamiento de documentación personal y la instalación de *software* ajenos a las funciones laborales.

Los sistemas de información, así como los servidores, dispositivos de red y demás servicios tecnológicos, guardarán registros de auditoría (historial de registro), los cuales contemplan, siempre y cuando sea posible:

- Identificación del usuario;
- Fecha y hora de la transacción;
- Dirección IP y nombre del dispositivo desde el cual se realizó la transacción;
- Tipo de transacción;
- Identificación de la transacción;
- Datos consultados, modificados o borrados;
- Intentos fallidos de conexión;

- Cambios en la configuración del sistema;
- Cambio o revocación de privilegios;
- Archivos a los que ha tenido acceso;
- Alarmas originadas por los sistemas de control;
- Desactivación de los mecanismos de protección.

6. Licenciamiento antivirus

Se mantiene activo el licenciamiento antivirus como una capa más de protección contra los programas malignos. El producto nos brinda capas contra la suplantación de identidad, protección contra ataques de día cero, protección contra programas de secuestro y actualización permanente sobre parches de seguridad.

7. Administración de cortafuegos

Se realiza la segmentación y habilitación de las redes por medio de equipos cortafuegos de seguridad perimetral donde se bloquean los intentos de intrusión a nuestra red y se contabilizan los inicios de sesión de nuestros usuarios, teniendo identificados los accesos a los sitios web y los ingresos a los diferentes sistemas institucionales.

8. Comunicaciones cifradas

En cuanto a la atención y respuesta a las emergencias de seguridad nacional, así como la coordinación interna de la Policía Nacional, se cuenta con un sistema de radiocomunicación de última generación con cifrado de seguridad para salvaguardar la integridad de nuestras comunicaciones.

Todas estas medidas adoptadas mejoran la protección de la información institucional y coadyuvan esfuerzos para evitar un ataque cibernético por no contar con medidas de protección para nuestro sistemas. A pesar de que en la actualidad no hay ningún sistema totalmente seguro, poniendo en práctica algunas de estas medidas disminuimos la brecha de vulnerabilidades informáticas y procuramos una gobernabilidad digital del ciberespacio a través de la identificación y los bloqueos de ataques cibernéticos.

Hungría

[Original: inglés]
[15 de mayo de 2020]

Apreciación general de las cuestiones relacionadas con el ciberespacio en el contexto de la seguridad internacional

En diciembre de 2019, 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, la Asamblea invita a los Estados Miembros a que sigan comunicando al Secretario General sus opiniones y evaluaciones sobre las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en esa esfera y el contenido de los conceptos mencionados en los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

Hungría acogería con beneplácito que se siguieran examinando de manera periódica las normas, reglas y principios voluntarios para el 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 y se crearan nuevos Grupos de Expertos Gubernamentales.

En 2018, Hungría apoyó las resoluciones de la Asamblea General 73/266 y 73/27 en virtud de las cuales se crearon, respectivamente, otro Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional y 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, como importantes medidas para hacer frente a las amenazas que plantea el uso de las tecnologías de la información y las comunicaciones (TIC).

Aunque seguimos con gran interés la labor de los anteriores Grupos de Expertos Gubernamentales, incluso durante la adopción de nuestra primera Estrategia Nacional de Ciberseguridad en 2013, esta es la primera vez que Hungría participa en las negociaciones. Desde su creación, Hungría estuvo representada en las reuniones oficiales primera y segunda del Grupo de Trabajo de Composición Abierta por su Representante Permanente ante la Organización para la Seguridad y la Cooperación en Europa (OSCE) (que también presidía el Grupo de Trabajo Oficioso sobre Seguridad Cibernética de la OSCE) y por el Coordinador para Cuestiones Cibernéticas del Ministerio de Relaciones Exteriores y Comercio, respectivamente. Hungría también participa activamente en las consultas relativas al proyecto de informe de la Presidencia del Grupo de Trabajo de Composición Abierta. En general, Hungría se adhiere a la posición de la Unión Europea.

Hungría apoya firmemente un sistema multilateral eficaz, sustentado en un orden internacional basado en normas, que logre hacer frente a los desafíos mundiales en el ciberespacio. Ejemplo de ello es nuestra participación en diferentes iniciativas intergubernamentales y de múltiples interesados y el apoyo prestado a esas iniciativas. Hungría reitera la aplicabilidad del derecho internacional vigente al comportamiento de los Estados en el ciberespacio, como se reconoce en los informes aprobados por consenso del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015. Sin embargo, el incumplimiento de las obligaciones en virtud del derecho internacional por parte de agentes estatales y no estatales sigue constituyendo una importante amenaza para la paz y la seguridad internacionales y para nuestra soberanía nacional, tanto en el mundo físico como en el ciberespacio. Por lo tanto, necesitamos ser capaces de disuadir y prevenir tanto los ataques convencionales como los no convencionales.

Apoyo a la Agenda para el Desarme

Hungría comparte las preocupaciones expresadas por el Secretario General sobre el creciente uso malintencionado de las TIC y, por lo tanto, apoya la promoción de un entorno pacífico de TIC como una prioridad clave establecida en la Agenda de Desarme anunciada por el Secretario General en mayo de 2018. Como reconocimiento de nuestro alto nivel de compromiso, la Oficina de Asuntos de Desarme de las Naciones Unidas ha indicado que Hungría apoya la medida 31 de la Agenda, destinada a fomentar la rendición de cuentas y el cumplimiento de las nuevas normas en el ciberespacio.

Hungría apoya los buenos oficios del Secretario General para prevenir la escalada de incidentes cibernéticos y para la puesta en marcha de cibernormas voluntarias, así como una mayor colaboración destinada a cerrar la brecha de conocimientos cibernéticos entre los Estados Miembros.

La ciberseguridad como cuestión de seguridad nacional

En abril de 2020, el Gobierno aprobó la nueva Estrategia Nacional de Seguridad de Hungría (adjunta a la Decisión 1163/2020 del Gobierno (IV. 21.)), sobre la base de la cual debe revisarse nuestra actual Estrategia Nacional de Ciberseguridad. La nueva Estrategia Nacional de Seguridad ofrece un panorama general de los cambios en las amenazas a la seguridad en el período posterior a 2012. Uno de sus principales objetivos es determinar, abordar y responder a los retos de seguridad que plantea el rápido desarrollo de las tecnologías de la información y las comunicaciones.

Se espera que el número y la sofisticación de los ciberataques sigan creciendo. Por lo tanto, el Gobierno de Hungría, en cooperación con otros interesados, hará todo lo que esté a su alcance para fortalecer sus capacidades a fin de protegerse contra los ciberataques malintencionados dirigidos contra nuestra infraestructura de información crítica y aumentar aún más la sensibilización pública sobre la ciberhigiene.

Abordar los desafíos causados por la propagación de la información falsa y la desinformación tanto en línea como fuera de línea es una prioridad clave, especialmente hoy en día, mientras seguimos luchando contra la pandemia de enfermedad por coronavirus (COVID-19). En una emergencia nacional, la información falsa puede ser muy perjudicial.

El desarrollo de cibercapacidades ofensivas y defensivas debe ser compatible con las obligaciones de un Estado en virtud del derecho internacional. De lo contrario, el uso de capacidades ofensivas en la esfera de las TIC puede contribuir a la militarización del espacio digital.

En nuestra opinión, las cibercapacidades que pueden suponer una amenaza para la seguridad y la estabilidad nacionales se consideran armas, cuyo uso puede llegar al umbral de un ataque armado al que los Estados también pueden reaccionar con una respuesta cinética como medio de autodefensa. Teniendo en cuenta los problemas de atribución en el entorno de las TIC, las autoridades públicas, en el caso de un incidente de TIC, deben actuar con la debida diligencia y considerar toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho y la naturaleza y el alcance de las consecuencias.

Cooperación internacional y otras iniciativas de múltiples interesados

En su calidad de miembro de la Unión Europea, Hungría participa activamente en la elaboración de un conjunto de instrumentos de ciberdiplomacia propios de la Unión Europea, a fin de coordinar la respuesta de esta a las actividades cibernéticas malintencionadas contra sus instituciones y sus Estados miembros que se originan fuera de la Unión Europea. Haciendo hincapié en la importancia de la cooperación internacional, apoyamos un mayor diálogo con nuestros socios estratégicos, aliados y otras organizaciones internacionales.

Ningún país u organización puede tener éxito por sí solo en la lucha contra las actuales amenazas a la seguridad. Esto hace que las asociaciones, en particular la cooperación entre la Unión Europea y la Organización del Tratado del Atlántico Norte (OTAN), sean hoy más importantes que nunca. No hay otra alternativa que continuar y profundizar esta cooperación en los próximos años. La lucha contra las amenazas híbridas (incluidas las amenazas a la ciberseguridad) es sin duda una de las principales esferas en las que las dos organizaciones deberían centrar sus esfuerzos.

Se prevé que los conflictos en el ciberespacio se intensificarán aún más en los próximos años y que la brecha de capacidad entre los países tecnológicamente avanzados y los países en desarrollo se seguirá ampliando. En julio de 2016, los

aliados reafirmaron el mandato defensivo de la OTAN y reconocieron el ciberespacio como un ámbito operacional que la OTAN debe defender. En julio de 2018, los aliados declararon una vez más la disposición de la OTAN a seguir adaptándose a la evolución de las ciberamenazas, que se ven afectadas tanto por agentes estatales como no estatales, incluidos los patrocinados por el Estado. Los Estados miembros de la OTAN acordaron integrar los efectos cibernéticos que afectan a la soberanía, proporcionados voluntariamente por los aliados, en el marco de una fuerte supervisión política. Reafirmando el mandato defensivo de la alianza, la OTAN declaró que estaba decidida a emplear una amplia gama de capacidades, incluidas las cibercapacidades, para disuadir todas las ciberamenazas, defenderse de ellas y contrarrestarlas. La OTAN se ha comprometido a seguir desarrollando su asociación con la industria y el mundo académico de todos los aliados para mantener el ritmo de los avances tecnológicos a través de la innovación.

El compromiso de Hungría con la ciberseguridad no es algo nuevo. El primer acuerdo internacional, y todavía único, sobre la lucha contra la ciberdelincuencia, denominado Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como el Convenio de Budapest, se acordó en Budapest en 2001 y, desde entonces, ha servido de guía para elaborar una amplia legislación nacional contra la ciberdelincuencia y como marco para la cooperación internacional. El tratado fue ratificado por la Ley LXXIX de 2004. Además de ser parte en el Convenio de Budapest, Hungría promueve activamente la adhesión de terceros países a dicho Convenio.

Como contribución nacional, desde 2017 el Representante Permanente de Hungría ha actuado como Presidente del Grupo de Trabajo Oficioso de la OSCE establecido en virtud de la decisión 1039 del Consejo Permanente sobre la elaboración de medidas de fomento de la confianza para reducir los riesgos de conflicto derivados del uso de las TIC. Hungría apoya los esfuerzos para estrechar la cooperación entre los procesos de las Naciones Unidas y otras organizaciones regionales pertinentes, como la OSCE. A nivel regional, subrayamos la importancia de aplicar el conjunto de medidas de fomento de la confianza adoptadas por la OSCE. También somos partidarios de aumentar la globalización de las medidas regionales de fomento de la confianza en el contexto del Grupo de Trabajo de Composición Abierta. Sin embargo, nuestro objetivo debería ser poner en práctica todas y cada una de las medidas regionales de fomento de la confianza con el mismo nivel de eficacia.

Hungría es uno de los pocos países con personal dedicado a la ciberdiplomacia. El Coordinador para Cuestiones Cibernéticas del Ministerio de Relaciones Exteriores y Comercio se encarga de las actividades de divulgación internacional sobre cuestiones relativas al ciberespacio en las relaciones bilaterales y multilaterales, incluidas las Naciones Unidas, la Unión Europea, la OSCE y otras iniciativas pertinentes de múltiples interesados, como el Foro Mundial de Competencia Cibernética. La ciberdiplomacia es un ámbito relativamente nuevo de nuestra cooperación internacional del que nuestro Gobierno puede beneficiarse, al tiempo que hace frente a las actividades cibernéticas malintencionadas.

Hungría contribuye a las actividades de creación de capacidad en terceros países. Como parte de esos esfuerzos, la ciberseguridad también desempeña un papel fundamental en la política de cooperación internacional para el desarrollo de Hungría, especialmente con respecto a los países asociados de África. Con ese fin, Hungría ha venido prestando asistencia para el desarrollo a Uganda en la esfera de la seguridad de la tecnología de la información con el objetivo de ayudarle a hacer frente a los desafíos del siglo XXI. La esfera de la seguridad cibernética es un elemento clave de la cooperación establecida en la Estrategia para África recientemente adoptada por

Hungría y su Estrategia de Cooperación Internacional para el Desarrollo para el período 2020-2025.

Además de participar en diferentes negociaciones intergubernamentales, el Gobierno de Hungría apoya iniciativas de múltiples interesados, como el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, en respuesta al llamamiento para una cooperación más profunda en la elaboración de normas, reglas y principios de comportamiento de los Estados en el ciberespacio. Decenas de organizaciones del sector privado de Hungría se unieron a nuestro Gobierno en estos esfuerzos. Hungría también apoya el Llamamiento de Christchurch para eliminar los contenidos terroristas y extremistas violentos en línea, que tiene repercusiones negativas en los derechos humanos y en nuestra seguridad colectiva.

Hungría comparte la opinión de que las organizaciones no gubernamentales (la sociedad civil, el mundo académico, el sector privado y la comunidad de las TIC) disponen de una serie de conocimientos técnicos o de los recursos necesarios para contribuir al desarrollo de un ciberespacio seguro y sostenible en el marco de sus propias funciones y responsabilidades. Los Estados desempeñan un importante papel en la promoción de esta coordinación y colaboración.

Indonesia

[Original: inglés]
[31 de mayo de 2020]

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

Indonesia cuenta con más de 170 millones de usuarios de Internet, lo que representa el 65 % de su población total. Las tecnologías de la información y las comunicaciones (TIC) han brindado a Indonesia oportunidades que son fundamentales para el logro de los Objetivos de Desarrollo Sostenible. Por otro lado, los desafíos en el ciberespacio también están aumentando. En 2019, Indonesia sufrió más de 220 millones de ciberataques, lo que obstaculizó el uso beneficioso del ciberespacio.

Indonesia está aplicando activamente múltiples medidas para aprovechar al máximo el potencial digital y hacer frente a las ciberamenazas mediante el fortalecimiento de los aspectos jurídicos y normativos de la infraestructura institucional, la creación de capacidad y la cooperación internacional.

Iniciativas nacionales

En 2017 se estableció la Agencia Nacional de Ciberseguridad y Criptografía como órgano centralizado de Indonesia en materia de asuntos relacionados con la ciberseguridad. En el marco de la Agencia, se ha establecido el Equipo Informático de Respuesta de Emergencia de Indonesia para dar una respuesta rápida a los incidentes cibernéticos dirigidos a las infraestructuras gubernamentales o privadas. También se ha creado un equipo de respuesta a incidentes de ciberseguridad en cada organismo público central y de distrito en las 34 provincias de Indonesia, para hacer frente a los incidentes cibernéticos y recuperarse de ellos.

Con miras a fortalecer el marco jurídico y normativo nacional, Indonesia promulgó la Ley de Información y Transacciones Electrónicas, así como la Hoja de Ruta Nacional de Comercio Electrónico para 2017-2019, que incluye medidas para asegurar las transacciones electrónicas y digitales. Las Directrices de Ciberdefensa de Indonesia se aprobaron mediante el Reglamento núm. 82 de 2014 del Ministerio

de Defensa. El sistema nacional de normalización de Indonesia también ha adoptado normas internacionales para la seguridad de las TIC, a saber, la ISO/IEC 27001 y la ISO 15408.

La ley de ciberseguridad de Indonesia se ha fijado como proyecto de ley prioritario para 2020, y el proceso legislativo está actualmente en curso. Indonesia también está redactando actualmente la estrategia nacional de ciberseguridad para 2020-2024, que abarca cinco pilares: la ciberresiliencia, el fortalecimiento del marco jurídico, la capacidad en materia de cibertecnología, el apoyo al crecimiento económico digital y la cooperación nacional e internacional.

Indonesia también se ha comprometido a seguir fortaleciendo la cooperación interna, en particular con las empresas de propiedad estatal, el sector privado y la industria para apoyar la creación de una cultura de ciberseguridad inclusiva. Desde 2018, el Gobierno de Indonesia inició la Campaña de Alfabetización sobre Ciberseguridad para promover el acceso seguro a Internet, la campaña contra los bulos y el ciberacoso, la ética de los medios sociales, la utilización responsable y la orientación a los padres sobre la seguridad de sus hijos en Internet.

Iniciativas internacionales

Mediante sus múltiples iniciativas, Indonesia sigue fomentando la cooperación mutua, las mejores prácticas y la capacidad para contribuir a la construcción de una estructura eficaz en materia de ciberseguridad que, en última instancia, podría adoptarse a nivel universal.

En lo que respecta a la participación multilateral a nivel mundial, Indonesia participa activamente 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, en particular en su calidad de Coordinador del Grupo de Trabajo sobre Desarme del Movimiento de Países No Alineados. Indonesia también figura actualmente entre los 25 miembros del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

En el plano regional, Indonesia participa en las medidas de fomento de la confianza en el marco de la Asociación de Naciones de Asia Sudoriental (ASEAN), entre otras cosas, apoyando el establecimiento de puntos de contacto en los órganos sectoriales de la ASEAN que se ocupan de las cuestiones cibernéticas en el marco de sus pilares de comunidad política y de seguridad y de comunidad económica, así como mediante el intercambio de información, la colaboración periódica en materia de ciberseguridad y los diálogos de los Estados miembros. La ASEAN también refuerza su cooperación en cuestiones de ciberseguridad mediante el establecimiento de un comité de coordinación entre pilares. Por conducto del Foro Regional de la ASEAN, el debate sobre las medidas de fomento de la confianza en el contexto de la ciberseguridad se ha ampliado más allá de la ASEAN para incluir también a otros países y asociados.

Además, Indonesia mantiene diálogos y cooperación bilaterales con diversos Estados y asociados. Indonesia seguirá impulsando de manera significativa los esfuerzos por fortalecer el comportamiento responsable de los Estados, así como la promoción de un entorno de TIC abierto, seguro, estable, accesible y pacífico.

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

El uso indebido del ciberespacio por agentes estatales y no estatales, incluidos los intermediarios, plantea riesgos para la paz y la seguridad internacionales, así como

para la estabilidad del país en las esferas política, económica y social. También se está produciendo un gran cambio en las TIC a nivel internacional para hacer frente a las implicaciones multidimensionales de la pandemia de la enfermedad por coronavirus (COVID-19). Los ciberactores malintencionados podrían intentar explotar, en particular, los sistemas de TIC y la difusión de información en el ciberespacio.

La comprensión mutua, la cooperación, la colaboración, las medidas de fomento de la confianza, la asistencia y la creación de capacidad son esenciales para fortalecer la seguridad y la estabilidad en el ciberespacio. Se deben apoyar los esfuerzos bilaterales, regionales y mundiales, a este respecto, que deben considerarse complementarios y no competidores.

Indonesia apoya la continuación del debate y la aplicación de normas no vinculantes de conformidad con el informe del Grupo de Expertos Gubernamentales de 2015. Indonesia reitera el papel fundamental que desempeñan las Naciones Unidas y las organizaciones regionales en la promoción del debate y la aplicación de 11 normas, medidas de fomento de la confianza y capacidades en materia de ciberseguridad, especialmente para reducir y cerrar la brecha digital entre los países.

Indonesia considera que las normas voluntarias y no vinculantes proporcionan un marco importante para el comportamiento responsable de los Estados. Si bien es necesario cerrar la brecha en cuestiones de ciberespacio sin gobierno, Indonesia alienta la creación de nuevas prácticas estatales consuetudinarias.

Indonesia está dispuesta a examinar la aplicación del derecho internacional vigente en el ciberespacio, incluida la posibilidad de la *lex specialis*. Indonesia subraya que la utilización del ciberespacio debe hacerse de conformidad con los principios jurídicos internacionales, especialmente los relacionados con el pleno respeto de la soberanía, la no intervención, el arreglo pacífico de controversias, los derechos humanos y la Carta de las Naciones Unidas.

Indonesia es partidaria de que todos los Estados hagan una declaración en la Asamblea General según la cual se abstendrían de militarizar el ciberespacio, lo que socava la paz y la seguridad internacionales y es contrario a los derechos y obligaciones de los Estados en virtud del derecho internacional.

Indonesia hace hincapié en la necesidad de aumentar la comprensión y profundizar el compromiso, en particular en el caso de los países y regiones que no han participado adecuadamente en el discurso y las medidas de ciberseguridad.

Irlanda

[Original: inglés]
[30 de mayo de 2020]

Irlanda acoge con beneplácito esta oportunidad de responder a la solicitud del Secretario General, de conformidad con el párrafo 2 de la resolución 74/28, relativa a la promoción de un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. Irlanda también apoya la presentación de la Unión Europea.

Nuestras sociedades y estados se han beneficiado de las tecnologías de la información y las comunicaciones (TIC), que han facilitado la comunicación, la educación, la innovación y la actividad económica, y han promovido la prosperidad. Sin embargo, en un mundo cada vez más interconectado, el uso indebido de estas poderosas tecnologías también puede tener repercusiones muy negativas, y el

aumento de las actividades cibernéticas malintencionadas, incluso durante la actual pandemia, preocupa enormemente a Irlanda. Estas actividades afectan a los ciudadanos y a su confianza en las instituciones. Sus efectos se sienten también en las sociedades y los Estados, donde pueden provocar conflictos o intensificar los ya existentes.

Las Naciones Unidas siguen siendo el principal foro para abordar los desafíos relacionados con el uso indebido de las TIC y las actividades cibernéticas malintencionadas, que repercuten en los tres pilares de la agenda de las Naciones Unidas: la paz y la seguridad, los derechos humanos y el desarrollo sostenible. Como economía con un importante sector de TIC, y como país profundamente comprometido con las Naciones Unidas, Irlanda seguirá apoyando a las Naciones Unidas en la promoción y el fomento de un comportamiento responsable de los Estados en el ciberespacio. Irlanda también seguirá colaborando activamente con los asociados de las Naciones Unidas y a nivel internacional para apoyar un ciberespacio abierto, libre y seguro, promover la libertad de expresión, asociación y reunión en línea, reducir el riesgo de conflicto y promover la paz, y velar por que los beneficios sociales y económicos del ciberespacio sean accesibles para todos, y apoyen en particular los Objetivos de Desarrollo Sostenible. Creemos que los progresos en la solución de los problemas que se plantean solo pueden sostenerse mediante la participación multilateral y de múltiples interesados, a lo que nos comprometemos a nivel nacional mediante iniciativas como el grupo de ciberseguridad Cyber Ireland, que se creó en 2019 con financiación del Gobierno y que reúne a múltiples interesados de la industria, el mundo académico y el Gobierno para examinar y promover la cooperación y la sensibilización sobre la educación y las oportunidades de carrera relacionadas con la cibernética, y para promover la innovación en el sector de la ciberseguridad de Irlanda. También hacemos extensivo este compromiso a nuestro enfoque internacional y, a este respecto, acogemos con satisfacción las iniciativas de las Naciones Unidas y otros foros para promover una cooperación y un diálogo más amplios, en particular mediante 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. Irlanda apoya también las reuniones del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional.

El enfoque de Irlanda con respecto a las cuestiones cibernéticas sigue basándose en nuestro compromiso con la aplicabilidad y el carácter central del derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional humanitario y las normas internacionales de derechos humanos. Irlanda también acoge con beneplácito el consenso alcanzado por la Asamblea General en 2015 en el sentido de que todos los Estados deben guiarse en su utilización de las TIC por el informe del Grupo de Expertos Gubernamentales de 2015, en el que se establecen 11 normas voluntarias y no vinculantes de comportamiento responsable de los Estados. Consideramos que esas normas, combinadas con el derecho internacional y complementadas con medidas de fomento de la capacidad para crear ciberresiliencia y facilitar un mayor acceso a las TIC, y con medidas de fomento de la confianza destinadas a reducir el riesgo de conflicto armado, proporcionan un marco sólido para promover un comportamiento positivo de los Estados en el ciberespacio. Las iniciativas de creación de capacidad en materia de TIC también pueden ayudar a cerrar la persistente brecha digital mundial, transformando la vida de las personas y las comunidades y promoviendo la prosperidad, contribuyendo al logro de los Objetivos de Desarrollo Sostenible y facilitando su consecución, incluso en lo que respecta a las cuestiones de género.

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

Estrategia Nacional de Ciberseguridad de Irlanda 2019-2024

En un ciberespacio interconectado, todos los Estados deben asegurarse de crear resiliencia contra los riesgos relacionados con la cibernética, tanto a nivel nacional como mundial. En la Estrategia Nacional de Ciberseguridad de Irlanda para 2019-2024[8] se establecen medidas y objetivos fundamentales a este respecto. La Estrategia apoya el objetivo de las Naciones Unidas de promover un comportamiento responsable de los Estados en el ciberespacio y de mantener la paz y la seguridad internacionales protegiendo a Irlanda, su población y su infraestructura nacional crítica de las amenazas a la ciberseguridad. También sustenta el compromiso internacional de Irlanda de apoyar un ciberespacio libre, abierto, pacífico y seguro. La política de ciberseguridad de Irlanda es aplicada por el Centro Nacional de Ciberseguridad, que contribuye al programa cibernético de las Naciones Unidas promoviendo el diálogo sobre cuestiones cibernéticas y colaborando con organismos asociados y otros interesados a nivel internacional para promover la confianza y la seguridad en el ciberespacio.

Los objetivos clave de la Estrategia de Ciberseguridad de Irlanda son los siguientes:

- Seguir mejorando la capacidad de Irlanda para detectar y responder a los incidentes de ciberseguridad y gestionarlos
- Detectar y proteger la infraestructura nacional crítica aumentando la resiliencia a los ciberataques
- Mejorar la resiliencia y la seguridad de los sistemas de tecnología de la información del sector público para proteger mejor los servicios de los que dependen los ciudadanos y sus datos
- Invertir en iniciativas educativas para preparar a la fuerza de trabajo para carreras avanzadas en el ámbito de la tecnología de la información y la ciberseguridad
- Concienciar sobre las responsabilidades de las empresas en lo que respecta a la seguridad de sus redes, dispositivos e información e impulsar la investigación y el desarrollo en materia de ciberseguridad en Irlanda, entre otras cosas facilitando la inversión en nuevas tecnologías
- Seguir colaborando con los asociados y las organizaciones internacionales para garantizar que el ciberespacio siga siendo abierto, seguro, unitario y libre y pueda facilitar el desarrollo económico y social y fomentar la capacidad a largo plazo
- Aumentar el nivel general de conocimientos y la sensibilización de los particulares sobre las prácticas básicas de ciberhigiene y apoyarlos en ese ámbito mediante la información y la capacitación

Libro Blanco sobre Defensa

En el *Libro Blanco sobre Defensa* de Irlanda (publicado en 2015[9] y actualizado en 2019[10]) se señalan los peligros que plantea las ciberactividades malintencionadas en el plano nacional e internacional, incluso para la infraestructura crítica y los

[8] Disponible en www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.
[9] Disponible en https://assets.gov.ie/21963/f1e7723dd1764a4281692f3f7cb96966.pdf.
[10] Disponible en www.gov.ie/en/publication/a519cf-white-paper-on-defence-update-2019/.

servicios fundamentales, y se reconoce también la forma en que los problemas cibernéticos pueden utilizarse indebidamente para socavar valores fundamentales, como la dignidad humana, la libertad y la democracia. El *Libro Blanco sobre Defensa* y la Estrategia Nacional de Ciberseguridad siguen informando el compromiso de Irlanda en materia de TIC y cuestiones cibernéticas.

Enfoques bilaterales, regionales y multilaterales

Irlanda sigue promoviendo el diálogo sobre las TIC y las cuestiones cibernéticas en su colaboración con otros Estados a nivel bilateral y en foros regionales y multilaterales.

Irlanda acoge con beneplácito la labor de la Organización para la Seguridad y la Cooperación en Europa (OSCE) y otras organizaciones regionales de todo el mundo en la promoción de medidas de fomento de la confianza.

Irlanda apoya las iniciativas estatales y no estatales que promueven la confianza, la seguridad y la paz en el ciberespacio, incluido el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio. Irlanda también apoya el Llamamiento de Christchurch para eliminar los contenidos terroristas y extremistas violentos en línea. Irlanda es miembro de la Freedom Online Coalition, una organización formada por 31 Estados que trabajan juntos para promover la libertad en Internet.

Irlanda también ha presentado un memorando de intención para unirse al Centro de Excelencia de Cooperación en Ciberdefensa de Tallin, a fin de contribuir a la colaboración para hacer frente a los desafíos en materia de ciberseguridad con socios afines. Irlanda se unirá al Centro como participante contribuyente (como miembro no perteneciente a la OTAN).

Promoción de la cooperación internacional en la Unión Europea

Irlanda sigue desempeñando un papel pleno y proactivo en la Unión Europea en lo que respecta a las cuestiones cibernéticas y colabora estrechamente con sus asociados de la Unión Europea para promover un ciberespacio abierto, libre, estable y seguro a nivel mundial que contribuya a la prevención de conflictos, en particular mediante las iniciativas en materia de ciberdiplomacia y el conjunto de instrumentos de ciberdiplomacia de la Unión Europea. Con miras a desarrollar su ciberresiliencia, Irlanda también participa en varias iniciativas de la Agencia Europea de Defensa.

Promoción de la cooperación internacional en las Naciones Unidas

En las Naciones Unidas, Irlanda apoya la 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 (véase más adelante) y ha contribuido activamente al 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. La Embajadora de Irlanda ante las Naciones Unidas también intervino en la reunión del Consejo de Seguridad con arreglo a la fórmula Arria sobre ciberestabilidad, prevención de conflictos y fomento de la capacidad, celebrada el 22 de mayo de 2020, y subrayó el compromiso de Irlanda de colaborar con las Naciones Unidas en una amplia gama de actividades en esta esfera, entre otras cosas utilizando las TIC y el ciberespacio para alcanzar los Objetivos de Desarrollo Sostenible, con especial referencia al Objetivo relativo a la igualdad de género.

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

Principios generales

Irlanda apoya un enfoque multilateral y tecnológicamente neutro para promover la ciberseguridad mundial, sustentado en un orden internacional basado en normas. Irlanda considera que los debates de las últimas reuniones del Grupo de Trabajo de Composición Abierta se han enriquecido gracias a la participación y las contribuciones de los interesados (en particular la sociedad civil, el mundo académico y los representantes técnicos y de la industria). Estas partes interesadas desempeñarán un papel cada vez más importante en el asesoramiento a los Estados sobre la evolución futura en el ámbito de las TIC y en el mantenimiento directo de un ciberespacio seguro y estable. Irlanda considera que una mayor participación de los interesados en futuras reuniones y otros debates sobre cuestiones cibernéticas es valiosa y necesaria y debería formalizarse.

Amenazas existentes y nuevas amenazas

La Estrategia Nacional de Ciberseguridad de Irlanda reconoce el impacto creciente y positivo de las TIC en el desarrollo económico y social, pero también pone de relieve el aumento de la ciberdelincuencia, del robo de propiedad intelectual y de la difusión de la desinformación, así como del uso de cibercapacidades ofensivas por parte de los Estados. La pandemia de enfermedad por coronavirus (COVID-19) ha demostrado nuestra dependencia de las TIC para trabajar y comunicarnos de manera flexible y segura y para mantener la actividad económica. Sin embargo, la pandemia también ha puesto de relieve las actividades de agentes malintencionados que aprovechan las vulnerabilidades, tanto técnicas como humanas, para cometer delitos cibernéticos, o para difundir desinformación, sembrando confusión, desconfianza y división. Irlanda observa con especial preocupación los recientes ciberataques contra los servicios sanitarios y médicos y servicios conexos. Esos ataques contra servicios de atención sanitaria y otros servicios esenciales ponen en peligro vidas. Junto con sus asociados de la Unión Europea, Irlanda ha condenado esos ataques y ha pedido a todos los Estados que ejerzan la debida diligencia y adopten medidas apropiadas contra quienes realicen esas actividades desde su territorio, de conformidad con el derecho internacional y los informes del Grupo de Expertos Gubernamentales aprobados por consenso de 2010, 2013 y 2015.

Derecho internacional

Irlanda cree firmemente que el derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional humanitario y las normas internacionales de derechos humanos, es aplicable al ciberespacio y constituye un elemento central de este. Los derechos humanos y las libertades fundamentales deben respetarse tanto en línea como fuera de ella. Habida cuenta del marco jurídico internacional existente, Irlanda ha expuesto sus reservas, en particular en las recientes reuniones del Grupo de Trabajo de Composición Abierta, en torno a los llamamientos para que se elabore un nuevo instrumento jurídico. Sin embargo, Irlanda acoge con beneplácito el diálogo en curso para promover un mayor entendimiento compartido sobre la aplicabilidad del derecho internacional vigente al uso de las TIC por parte de los Estados.

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

Irlanda apoya las normas, reglas y principios voluntarios y no vinculantes para el comportamiento responsable de los Estados que figuran en el informe del Grupo de Expertos Gubernamentales de 2015 y acoge con beneplácito el acuerdo por consenso de la Asamblea General de que todos los Estados se guíen por el informe en

su uso de las TIC. Estas normas promueven la estabilidad y la seguridad en el entorno mundial de las TIC y pueden contribuir al mantenimiento de la paz internacional. La Estrategia Nacional de Ciberseguridad de Irlanda y la política irlandesa reflejan estas normas, reglas y principios, en particular en relación con el fomento de la capacidad sostenible. Irlanda ha pedido, en el seno de las Naciones Unidas, que se siga elaborando una orientación sobre la forma en que estas normas existentes, respaldadas por consenso por todos los Estados Miembros, podrían aplicarse y ponerse en práctica.

Medidas de fomento de la confianza

Irlanda contribuye proactivamente a los debates sobre las TIC y la ciberseguridad y los promueve en reuniones y foros bilaterales, regionales y multilaterales, en particular en el contexto de la paz y la seguridad mundiales, el desarrollo sostenible y los derechos humanos. Irlanda reconoce la amplia labor realizada por las organizaciones regionales y las iniciativas de los interesados estatales y no estatales, incluido el Llamamiento de París, en la promoción de la confianza, y apoya ampliamente las propuestas de establecer mecanismos para compartir las mejores prácticas en materia de medidas de fomento de la confianza en apoyo de futuras iniciativas.

Medidas de creación de capacidad

La Estrategia Nacional de Ciberseguridad de Irlanda incluye el compromiso de adoptar nuevas medidas de creación de capacidad sostenible. Irlanda también valora un enfoque multilateral y de múltiples interesados para crear resiliencia en todos los Estados contra la ciberactividad malintencionada y para reducir las vulnerabilidades, proteger la infraestructura crítica y hacer que todos los Estados se beneficien plenamente del acceso a las TIC. Irlanda también cree que es fundamental que todos los Estados y los principales interesados puedan participar en los debates mundiales sobre cuestiones cibernéticas. En ese sentido, Irlanda patrocinó la reunión oficiosa entre períodos de sesiones del Grupo de Trabajo de Composición Abierta, celebrada del 2 al 4 de diciembre de 2019, en la que los Estados se reunieron con las partes interesadas, incluidos representantes de organizaciones no gubernamentales y de la sociedad civil, expertos técnicos, investigadores y académicos, y el sector privado. Irlanda también apoya firmemente los esfuerzos para cerrar la brecha digital de género. Irlanda acogería con agrado que se establecieran vínculos más estrechos entre los futuros debates e iniciativas de las Naciones Unidas en materia de fomento de la capacidad y los Objetivos de Desarrollo Sostenible y la agenda sobre las mujeres y la paz y la seguridad.

Italia

[Original: inglés]
[29 de mayo de 2020]

Introducción

Italia se adhiere a las posiciones expresadas por la Unión Europea en su contribución al informe y desea proporcionar al Secretario General la siguiente información nacional.

A los efectos del presente informe, Italia no utilizará la expresión “seguridad de la información”, que no se utiliza en el ordenamiento jurídico italiano. Se emplean otras expresiones, como “ciberseguridad” o “seguridad de las redes y los sistemas de información”, que son preferibles. La libertad de expresión —tanto en línea como fuera

de ella— está reconocida por la legislación fundamental italiana y por el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, ratificado por Italia en 1978.

Según el Decreto del Primer Ministro italiano de 17 de febrero de 2017, que contiene directrices para la protección del ciberespacio y la seguridad de las tecnologías de la información y las comunicaciones a nivel nacional, el término "ciberseguridad" se refiere a la protección del ciberespacio garantizada mediante medidas de seguridad físicas, lógicas y de procedimiento adecuadas con el fin de prevenir y contrarrestar los hechos, ya sean intencionados o accidentales, que entrañen la adquisición y transferencia indebidas de datos, la modificación o destrucción ilegítima de datos, o el control indebido, el daño, la destrucción o el bloqueo del funcionamiento normal de las redes y los sistemas de información o sus componentes.

Asimismo, la expresión "seguridad de las redes y los sistemas de información" se refiere a la capacidad de una red o un sistema de información para resistir, con un cierto nivel de confidencialidad, cualquier acción que tenga por objeto la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados y de los servicios conexos disponibles o accesibles a través de esa red o ese sistema de información, según se define en el Decreto Legislativo 65/2018 por el que se incorpora la Directiva de la Unión Europea sobre la seguridad de las redes y sistemas de información.

Iniciativas para reforzar la ciberseguridad a nivel nacional: marco institucional y normativo

En diciembre de 2013, Italia aprobó el Marco Estratégico Nacional para la Ciberseguridad, en el que se toma nota de las amenazas crecientes y en evolución que plantea el uso de las tecnologías de la información y las comunicaciones (TIC) y que tiene por objeto aumentar la capacidad y la resiliencia cibernéticas de Italia. En los siguientes planes de acción nacionales, el último de los cuales se publicó en marzo de 2017 y se aprobó de conformidad con el mencionado Decreto del Primer Ministro de 17 de febrero de 2017, se establecen varias medidas, elementos y prioridades para la aplicación del Marco Estratégico.

En el Decreto del Primer Ministro se define la arquitectura nacional de ciberseguridad y su gobernanza, y se establece, en el Departamento de Información para la Seguridad, una Junta para la Seguridad Cibernética encargada de prevenir una cibercrisis nacional y prepararse para ella, así como de coordinar las actividades de respuesta y recuperación que deben llevar a cabo los sectores público y privado en cumplimiento de las decisiones del Primer Ministro.

La Junta para la Seguridad Cibernética consta de una Secretaría y de una junta mixta presidida por el Director General Adjunto de Cibernética del Departamento de Información para la Seguridad y está integrada por representantes de la comunidad de la información (el Departamento de Información para la Seguridad, la Agencia de Información y Seguridad Externa y la Agencia de Información y Seguridad Interna), el Asesor Militar del Primer Ministro, los Ministerios de Relaciones Exteriores y Cooperación Internacional, Asuntos Internos, Justicia, Defensa, Economía y Finanzas, y Desarrollo Económico, el Departamento de Protección Civil y la Agencia para la Italia Digital. Un representante de la Oficina Central de Asuntos Secretos del Departamento de Información para la Seguridad se une a la Junta siempre que se trata un hecho que pone en peligro los sistemas de información clasificada.

En caso de una cibercrisis nacional, la Junta también puede incluir representantes del Ministerio de Salud, el Ministerio de Infraestructura y Transporte y el Departamento de Bomberos. El Primer Ministro, sobre la base de la información

proporcionada por la Junta para la Seguridad Cibernética, puede declarar una situación de cibercrisis cuando un acontecimiento cibernético, por su escala, intensidad o naturaleza, no pueda ser abordado por la oficina correspondiente, sino que requiera un enfoque conjunto y coordinado, garantizado por la Junta para la Seguridad Cibernética.

Después del Decreto del Primer Ministro se aprobaron otras leyes, a saber:

- El Decreto Legislativo 65/2018, que incorpora la Directiva de la Unión Europea sobre la seguridad de las redes y sistemas de información y designa al Departamento de Información para la Seguridad como punto de contacto único para los sistemas de redes e información
- El Perímetro Nacional de Seguridad Cibernética (Ley 133/2019), que entró en vigor en noviembre de 2019, se aplica a las entidades nacionales públicas y privadas que desempeñan funciones esenciales o prestan servicios esenciales para la realización de actividades consideradas vitales para los intereses nacionales de Italia. Las entidades públicas y privadas se incluyen en el "perímetro" según el principio de "prioridad progresiva para la seguridad nacional". La ley abarca las redes, los sistemas y los servicios de tecnología de la información que son propiedad de las entidades mencionadas o que son explotados por ellas y que podrían afectar a la seguridad nacional. La ley establece lo siguiente:
  - La notificación de incidentes, a fin de garantizar un flujo de información inmediato hacia las estructuras pertinentes encargadas de la prevención, preparación y gestión de las actividades cibernéticas, a saber, la Junta para la Seguridad Cibernética y el Equipo de Respuesta a Incidentes de Seguridad Informática, que forman parte del Departamento de Información para la Seguridad
  - Medidas de seguridad que abarcan cuestiones, procesos y procedimientos de organización, incluida la adquisición de TIC
  - El examen tecnológico de los productos y servicios de TIC que entran en categorías específicas y están relacionados con los bienes o entidades incluidos en el perímetro. De conformidad con la ley, todo operador que desee adquirir esos artículos deberá informar al Centro Nacional de Evaluación y Certificación que, a su vez, podrá realizar evaluaciones preliminares, imponer condiciones y exigir pruebas de los equipos o programas informáticos. En este último caso, las convocatorias de licitación y los contratos correspondientes incluirán una cláusula de suspensión de las políticas de cancelación, en relación con los requisitos que deben cumplirse o con los resultados positivos de las pruebas exigidas por el Centro Nacional de Evaluación y Certificación
  - Las actividades de inspección y sanción de los agentes públicos y privados serán llevadas a cabo respectivamente por el Presidente del Consejo de Ministros y el Ministro de Desarrollo Económico.

En caso de que se produzca un riesgo grave e inminente para la seguridad nacional relacionado con las redes, los sistemas y los servicios de tecnología de la información, el Primer Ministro podrá dar instrucciones para que se apaguen o suspendan parcial o totalmente uno o más dispositivos o productos instalados en las redes o sistemas o relacionados con la prestación de servicios. La decisión está sujeta a la deliberación previa del Comité Interministerial para la Seguridad de la República y es válida durante el tiempo estrictamente necesario para eliminar o mitigar la amenaza, de acuerdo con el principio de la proporcionalidad.

- El Decreto Ley 22/2019 convertido en Ley 41/2019 (artículo 1), que complementa el Decreto Ley 21/2012 “Golden Power” convertido en Ley 56/2012 sobre facultades excepcionales en los sectores de la defensa y la seguridad nacional, así como para actividades estratégicamente importantes en los sectores de la energía, el transporte y las comunicaciones, incluye los servicios de comunicación electrónica de banda ancha basados en tecnologías 5G entre las actividades estratégicamente importantes para la defensa y la seguridad nacionales. De acuerdo con las últimas disposiciones, los contratos o acuerdos sobre la adquisición de bienes o servicios para la planificación, ejecución, mantenimiento y gestión de redes relacionadas con los servicios de comunicación electrónica de banda ancha basados en tecnologías 5G, o la adquisición de componentes de tecnología de alta intensidad útiles para la ejecución o gestión mencionadas, deben ser notificados a la Junta “Golden Power” establecida en el marco de la Presidencia del Consejo de Ministros, siempre que participen entidades ajenas a la Unión Europea. La razón de ello es permitir el ejercicio del poder de veto o imponer prescripciones y condiciones específicas, que pueden modificarse o combinarse con medidas adicionales, incluida la sustitución de productos y equipo, si el Centro Nacional de Evaluación y Certificación detecta la presencia de vulnerabilidades que puedan poner en peligro la integridad y la seguridad de las redes y sus datos.

Ciberdefensa

El Libro Blanco para la Seguridad y la Defensa Internacionales de 2015 reconoce la necesidad de proteger y defender el ámbito cibernético, incluso mediante el establecimiento de capacidades operacionales defensivas específicas a fin de preservar la solidez de las estructuras políticas, económicas y sociales. Según el Documento de Planificación Plurianual del Ministerio de Defensa para los años 2019-2021, el ciberespacio debe ser protegido y defendido de los ataques a los servicios de red o informáticos y a las infraestructuras críticas. En los últimos años, el Ministerio de Defensa ha realizado una serie de reformas para reforzar su protección, así como su resiliencia y posición.

Entre otras cosas, el Ministerio de Defensa de Italia estableció en 2017 el Comando Conjunto de Operaciones Cibernéticas, un comando militar encargado de planificar, dirigir y llevar a cabo operaciones cibernéticas, con el fin de detectar y neutralizar las amenazas y los ataques contra las redes, los sistemas y los servicios del Ministerio de Defensa dentro del país, así como en los teatros de operaciones fuera de las fronteras italianas.

El Comando Conjunto de Operaciones Cibernéticas se ha integrado recientemente en el recién creado Comando para las Operaciones en Red, con el objetivo de desarrollar una cadena de mando más directa y garantizar una mayor eficiencia y coordinación entre todos los departamentos de ciberseguridad pertinentes que existen en los sectores de defensa (Fuerza Aérea, Ejército y Marina). El Comando para las Operaciones en Red apoya al Comando de Operaciones Conjuntas de Italia, y tiene la tarea de llevar a cabo operaciones defensivas para proteger al Ministerio de Defensa italiano y su aparato militar de incidentes y ataques cibernéticos.

Además, el Comando para las Operaciones en Red:

- Se encarga de la ciberseguridad y la ciberdefensa de las redes del Ministerio de Defensa, que asegura a través del Equipo Informático de Respuesta de Emergencia, que se encarga de vigilar la ciberactividad y de prevenir y gestionar los incidentes y emergencias que afectan al sector de la defensa;

- Está llevando a cabo un estudio para definir el marco jurídico en los teatros de operaciones, respetando estrictamente el derecho internacional y el derecho internacional humanitario. Ese estudio tendrá por objeto definir las normas y las reglas de enfrentamiento mínimas para apoyar las operaciones mediante actividades realizadas en el ciberespacio. La necesidad de un marco jurídico se deriva, entre otras cosas, de las numerosas actividades y ejercicios nacionales e internacionales realizados en los últimos años, incluso en el marco de la Organización del Tratado del Atlántico Norte (OTAN).

Se ha creado un laboratorio cibernético en el seno del Comando Conjunto de Operaciones Cibernéticas con el fin de desarrollar herramientas para investigar las vulnerabilidades cibernéticas y organizar actividades de capacitación.

Otras actividades incluyen ensayos preliminares para impartir capacitación técnica cibernética en la Escuela de Telecomunicaciones de las Fuerzas Armadas italianas y la colaboración con muchas universidades italianas en la esfera de la ciberseguridad.

Iniciativas para promover la cooperación internacional en la esfera de la ciberseguridad, en particular en relación con los informes del Grupo de Expertos Gubernamentales

Según el artículo 10 de la Constitución italiana, el sistema jurídico italiano se ajusta a las normas generalmente reconocidas del derecho internacional.

Por consiguiente, Italia se compromete a promover la aplicación del derecho internacional vigente en el ciberespacio, incluida la Carta de las Naciones Unidas en su totalidad, también de conformidad con la posición de la Unión Europea según la contribución mencionada; el cumplimiento de las reglas, normas y principios de comportamiento responsable de los Estados establecidos por 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 2015 y los grupos anteriores; el desarrollo de medidas de fomento de la confianza y programas de creación de capacidad; y la gobernanza de Internet basada en un enfoque de múltiples interesados.

Italia apoya el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio en lo que respecta a la aplicación de medidas de cooperación para reducir los riesgos para la estabilidad del ciberespacio y para fomentar la confianza y la capacidad. Italia es también uno de los signatarios del Llamamiento de Christchurch para eliminar los contenidos terroristas y extremistas violentos en línea.

La promoción de las actividades de creación de capacidad con terceros países forma parte de nuestra estrategia nacional de ciberseguridad y se lleva a cabo de conformidad con las Conclusiones del Consejo sobre las directrices de la UE para la creación de capacidad externa, aprobadas por el Consejo de Asuntos Generales de la Unión Europea en su 3629ª reunión, celebrada el 26 de junio de 2018. Las actividades de creación de capacidad con terceros países se centran principalmente en el intercambio de información y mejores prácticas, especialmente en lo que respecta a la respuesta a incidentes de seguridad informática, la educación y la capacitación.

La participación en foros internacionales y el apoyo al cumplimiento de normas de comportamiento responsable de los Estados en el ciberespacio son también una parte esencial de la estrategia nacional de ciberseguridad de Italia. La cooperación internacional en la esfera de la ciberseguridad, incluso con respecto a los informes del Grupo de Expertos Gubernamentales, también se examina, cuando procede, en nuestros diálogos o consultas bilaterales y multilaterales. Los principales foros multilaterales en los que Italia contribuye activamente a mejorar la cooperación en el

ciberespacio son las Naciones Unidas, la Unión Europea, la OTAN, la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Consejo de Europa y el Grupo de los Siete.

Con respecto a este último, los días 10 y 11 de abril de 2017 Italia celebró la Reunión Ministerial del Grupo de los Siete sobre Asuntos Exteriores, en la que se aprobó la Declaración del G7 sobre el comportamiento responsable de los Estados en el ciberespacio. La Declaración exhorta a todos los Estados a que se guíen en su uso de las TIC por los informes acumulativos de los Grupos de Expertos Gubernamentales de las Naciones Unidas en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

Durante la Presidencia italiana de la OSCE en 2018, Italia apoyó activamente la aplicación efectiva de las medidas de fomento de la confianza de la OSCE en la esfera de la seguridad de las comunicaciones y la información por parte de los Estados participantes, entre otras cosas organizando un debate basado en escenarios sobre su utilización en el caso de un incidente cibernético internacional, de forma paralela a la Conferencia de los miembros de la OSCE sobre seguridad cibernética y de las TIC celebrada en Roma los días 27 y 28 de septiembre de 2018. En 2019, Italia, durante su Presidencia del Grupo de Contacto con los Socios Asiáticos de la OSCE, organizó la 20ª Conferencia OSCE-Asia sobre cómo lograr la seguridad integral en la era digital: perspectivas de la OSCE y sus socios asiáticos, que se celebró en Tokio los días 2 y 3 de septiembre de 2019. Italia también apoyó varios proyectos de la OSCE sobre creación de capacidad en la esfera de las cibertecnologías y las TIC, como el proyecto de capacitación subregional sobre la función de las tecnologías de la información y las comunicaciones (TIC) en el contexto de la seguridad regional e internacional, celebrada en Atenas los días 7 y 8 de febrero de 2019.

Italia participa activamente en las actividades del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y apoya la labor realizada por el actual Grupo de Expertos Gubernamentales y por los grupos anteriores. Italia recuerda también que en la resolución 70/237 de la Asamblea General se acogen con beneplácito las conclusiones de los anteriores grupos de expertos gubernamentales que figuran en los informes de 2013 y 2015 y se exhorta a los Estados Miembros a que se guíen por el informe de 2015 en su uso de las tecnologías de la información y las comunicaciones.

La reciente creación de un departamento que se ocupa de la ciberseguridad y las políticas cibernéticas en el Ministerio de Relaciones Exteriores y Cooperación Internacional de Italia tiene por objeto seguir reforzando y promoviendo nuestra acción diplomática y la cooperación internacional en este ámbito.

Japón

[Original: inglés]
[31 de mayo de 2020]

El Japón acoge con beneplácito la oportunidad de responder a la resolución 74/28 de la Asamblea General sobre la promoción de un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.

1. 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 y la Ley Enmendada sobre la Protección de la Información Personal. El Gobierno también ha adoptado una política de creación de una sociedad centrada en el ser humano 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 y son ahora 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 un 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 especial, el brote de la enfermedad por coronavirus (COVID-19) parece estar acelerando la tendencia de la humanidad a depender cada vez más de las tecnologías de la información y las comunicaciones (TIC), al tiempo que acentúa los riesgos y los problemas causados por el uso malintencionado de las TIC. Existe una creciente preocupación por los informes de ciberataques y actividades cibernéticas malintencionadas que se aprovechan de la crisis, incluidos los programas secuestradores que atacan a las instituciones médicas y las autoridades, así como los ataques de negación de servicio distribuidos contra instalaciones de investigación médica. 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, y consciente de la situación deseada para 2020 y años posteriores, el Japón no escatimará esfuerzos en relación con las medidas de ciberseguridad, aclarando su visión básica de la ciberseguridad, detectando los nuevos problemas que deben abordarse y adoptando medidas de rápida aplicación.

Medidas adoptadas a nivel 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 cuando sea necesario. Además, el Gobierno participará activamente en los debates internacionales para abordar las cuestiones relacionadas con la ciberseguridad que han surgido con el brote de COVID-19.

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 de respuesta, 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 los mismos 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 apropiada.

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 ciberataques. Debido al anonimato y al carácter secreto de los ciberataques, existe el riesgo de que estos aumenten involuntariamente las tensiones entre los Estados. 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 de Asia Sudoriental (ASEAN) en la esfera de la ciberseguridad, 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 críticas en esos Estados, así como el desarrollo racional de la utilización del ciberespacio en esos Estados. Al mismo tiempo, la creación de capacidades también está directamente relacionada 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 el primer país asiático que ha ratificado 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.

2. 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 TIC 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 las 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 nación 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 e impedir que se obtengan beneficios de los actos cibernéticos malintencionados. En este contexto, los miembros del Grupo deberían alentar sistemáticamente 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 a que cooperen en apoyo de las actividades de creación de capacidad nacional para aplicar las normas y recomendaciones antes mencionadas, incluso mediante el proceso del próximo Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta.

México

[Original: español]
[29 de mayo de 2020]

Las tecnologías de la información y los nuevos desarrollos en materia de telecomunicaciones han ampliado el espectro de posibilidades para el desarrollo sostenible y para alcanzar un mundo de derechos, de equidad y de inclusión. Garantizar el uso pacífico y para el bienestar colectivo de esas tecnologías es hoy una obligación para toda la comunidad internacional.

Las discusiones en las Naciones Unidas sobre la estabilidad en el ciberespacio, la ciberseguridad y la gobernanza del ciberespacio, y en particular los informes generados por el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional para promover el comportamiento responsable de los Estados en el ciberespacio, marcan las pautas para avanzar hacia un ciberespacio abierto, libre, estable y seguro.

En línea con esos antecedentes, el Gobierno de México presenta este informe convencido del valor de las resoluciones aprobadas por la Asamblea General en la materia y de que la vía multilateral es la única que podrá garantizar, con visión de largo plazo, los usos legítimos y pacíficos del ciberespacio, la resiliencia en el entorno digital, las posibilidades de las tecnologías de la información como habilitadoras del desarrollo sostenible y la protección de los derechos humanos en el ciberespacio.

1. Esfuerzos realizados a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este campo

El Gobierno de México ha consolidado los siguientes mecanismos de coordinación nacional en materia de seguridad de la información y órganos de respuesta:

a) Comité Especializado en Seguridad de la Información

Se trata de un órgano colegiado interagencial encargado del desarrollo de la política de seguridad de la información aplicable a las instancias de seguridad nacional y de verificar su adecuada aplicación en México. En este Comité están representadas las instituciones mexicanas federales encargadas de la seguridad nacional, la seguridad pública, las telecomunicaciones, el sector financiero y la política exterior. Entre las actividades que se han consolidado desde este Comité se encuentran el diseño y actualización de la estrategia nacional de ciberseguridad, ejercicios de respuesta a incidentes informáticos y la realización de actividades de concientización en materia de seguridad de la información, entre otros.

b) Centro Nacional de Respuesta a Incidentes Cibernéticos

Dentro de la estructura institucional de la nueva Guardia Nacional de México, esta instancia se encarga de vigilar la integridad de la infraestructura tecnológica estratégica del país. El Centro Nacional opera áreas especializadas en temas de prevención e investigación de conductas ilícitas a través de medios informáticos y monitorea las redes para identificar conductas constitutivas de delito, efectuando actividades de ciberseguridad para reducir y mitigar los riesgos de amenazas y ataques cibernéticos. De igual forma, implementa programas de desarrollo científico y tecnológico en materia cibernética.

c) Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información

Se ha constituido como mecanismo de coordinación para dar respuesta efectiva a incidentes de seguridad de la información en el sector financiero en el que participan la autoridad nacional de procuración de justicia, las autoridades financieras nacionales y las asociaciones gremiales financieras de México, cuya finalidad es dar respuesta efectiva a incidentes que afectan de manera directa al sector financiero.

En el ámbito nacional, México ha realizado las acciones que se indican a continuación para fortalecer la seguridad de la información en años recientes.

El Gobierno de México, por conducto de la Secretaría de Seguridad y Protección Ciudadana, organiza anualmente la Semana Nacional de la Ciberseguridad. Este evento tiene como propósito servir como un espacio de diálogo a favor de la seguridad cibernética, promoviendo una alianza entre los sectores involucrados para preservar un entorno digital seguro y resiliente. Asimismo, busca generar conciencia en la ciudadanía sobre tecnologías de la información y seguridad digital, a través de conferencias, paneles de discusión, capacitaciones, talleres, seminarios web y actividades lúdicas.

Desde 2018, el Gobierno de México, en asociación con la Organización de los Estados Americanos (OEA) y Trend Micro, realiza anualmente el evento denominado “Cyberwomen Challenge”. Esta actividad tiene por objeto promover la igualdad de género en las actividades relacionadas con la protección y la respuesta a las amenazas a la ciberseguridad, así como construir y fortalecer las capacidades institucionales en este ámbito.

Durante 2019, la Secretaría de Comunicaciones y Transportes coordinó la organización de mesas de trabajo sobre ciberseguridad, en las que participaron más de 5.000 personas de los centros de inclusión digital que opera la Secretaría de Comunicaciones y Transportes (ubicados en todo el país). Esta actividad tuvo como objetivo identificar comportamientos riesgosos en el uso de los servicios de telecomunicaciones y radiodifusión. La información recopilada a través de esta actividad sirvió como insumo para el informe titulado “Hábitos de los usuarios en ciberseguridad en México 2019”.

A partir de los resultados de dicho reporte se desarrolló un simulador con el apoyo de la OEA y el Gobierno de Reino Unido. El simulador es una herramienta que permitirá a los participantes experimentar amenazas de ciberseguridad simuladas, en un entorno interactivo, para evaluar su capacidad para responder a ellas y proporcionar asesoramiento sobre las mejores maneras de protegerse.

Adicionalmente, con el propósito de contribuir a fortalecer la cooperación internacional y el comportamiento responsable de los Estados en el ciberespacio, México participa en los siguientes foros, mecanismos e iniciativas multilaterales y regionales:

a) Primera Comisión de la Asamblea General de las Naciones Unidas

México participa 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, que se estableció en seguimiento a la resolución 73/27 de la Asamblea General.

Asimismo, un experto gubernamental de México participa en el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, que se conformó en seguimiento a la resolución 73/266.

México ha buscado que ambos procesos trabajen de manera complementaria, reconociendo asimismo que ambos continúan construyendo sobre la base de las labores de los grupos de expertos gubernamentales anteriores y sus informes adoptados por consenso por la Asamblea General.

b) Grupo de amigos sobre tecnologías digitales

Para México es muy importante diseñar y colaborar en acciones relativas a las tecnologías digitales, especialmente aquellas que apoyen la instrumentación de los Objetivos de Desarrollo Sostenible y sus metas, mediante el buen uso de las tecnologías de la información y las telecomunicaciones. Consistente con esta visión, desde noviembre de 2019, México copreside, junto con Finlandia y Singapur, el Grupo de Amigos sobre Tecnologías Digitales que tiene como objetivo fomentar un diálogo inclusivo con todos los actores interesados para analizar los vínculos entre tecnologías digitales y desarrollo sostenible y hablar de cooperación internacional en el tema de manera transversal.

c) Panel de Alto Nivel sobre la Cooperación Digital

En seguimiento a las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital, México encabezó junto con la Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres (ONU-Mujeres) el grupo para proponer medidas específicas para instrumentar las recomendaciones 1C y 1D, sobre la inclusión digital y métricas al respecto.

d) Unión Internacional de Telecomunicaciones

México participa en las iniciativas que la Unión Internacional de Telecomunicaciones coordina en materia de seguridad de la información y ciberseguridad, tales como la Agenda sobre Ciberseguridad Global y el Índice Mundial de Ciberseguridad.

En cuanto a la Agenda sobre Ciberseguridad Global, para México resulta una importante iniciativa que contribuye al propósito de construir un entorno digital más seguro y resiliente, además de que posee una valía intrínseca al considerar la participación de todos los actores relevantes, incluyendo a los Estados, al sector privado, a la sociedad civil y a la academia.

e) Organización de los Estados Americanos

México participa y colabora activamente con el programa de ciberseguridad del Comité Interamericano contra el Terrorismo de la OEA, el cual fomenta el desarrollo de políticas, el desarrollo de capacidades, la investigación y la divulgación en materia de ciberseguridad en el continente americano.

Asimismo, el Centro Nacional de Respuesta a Incidentes Cibernéticos participa en la red hemisférica de equipos de respuesta a incidentes de seguridad informática

de las Américas, que se enmarca en el trabajo del programa de ciberseguridad del Comité Interamericano contra el Terrorismo de la OEA.

México también participa en el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio del Comité Interamericano contra el Terrorismo de la OEA. Como resultado de los trabajos de este Grupo, que se estableció en 2018, se han adoptado las siguientes medidas de fomento de la confianza:

- Proporcionar información sobre políticas nacionales de ciberseguridad, como estrategias nacionales, libros blancos, marcos legales y otros documentos que cada Estado miembro considere relevantes;
- Identificar un punto de contacto nacional a nivel de políticas capaz de discutir las implicaciones de las amenazas cibernéticas hemisféricas;
- Designar puntos de contacto, en caso de no existir, en los ministerios de relaciones exteriores con el propósito de facilitar el trabajo en materia de cooperación y diálogos internacionales sobre ciberseguridad y ciberespacio;
- Desarrollar y fortalecer la generación de capacidades mediante actividades tales como seminarios, conferencias y talleres en ciberdiplomacia para funcionarios públicos y privados;
- Fomentar la incorporación de los temas de ciberseguridad y ciberespacio en los cursos de formación básica y capacitación a diplomáticos y funcionarios de los ministerios de relaciones exteriores y otras agencias de gobierno;
- Fomentar la cooperación y el intercambio de mejores prácticas en ciberdiplomacia, ciberseguridad y ciberespacio, a través de, por ejemplo, el establecimiento de grupos de trabajo, otros mecanismos de diálogo y la suscripción de acuerdos entre los Estados.

f) Foro Mundial de Competencia Cibernética

México participa en este Foro desde 2015, el cual busca el desarrollo de capacidades en materia de ciberseguridad. Los temas de interés de México son la prevención de ataques cibernéticos; la protección de datos; la prevención de delitos cibernéticos (incluyendo pornografía infantil y delitos similares); los esfuerzos de gobierno electrónico y estrategias digitales; la protección de infraestructura crítica; los usos pacíficos de las TIC e Internet; y la aplicabilidad del derecho internacional al ciberespacio.

g) Foro de Respuesta a Incidentes y Equipos de Seguridad

El Centro Nacional de Respuesta a Incidentes Cibernéticos forma parte del Foro de Respuesta a Incidentes y Equipos de Seguridad, un foro global donde convergen y colaboran equipos de respuesta a incidentes cibernéticos de todo el mundo. Ello permite generar y fortalecer líneas de investigación que, en colaboración con las policías cibernéticas de otras naciones, logre la identificación y ubicación de probables responsables de ataques cibernéticos.

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

En línea con las afirmaciones de los informes previos del Grupo de Expertos Gubernamentales, México considera que el derecho internacional es aplicable al ciberespacio. Para la instrumentación de esta afirmación el Gobierno de México ha encabezado esfuerzos internamente para consolidar como posición que la aplicación del derecho internacional se refiere a la Carta de las Naciones Unidas, al derecho

internacional de los derechos humanos, al derecho internacional humanitario, a las normas aplicables de derecho internacional consuetudinario e incluso a la jurisprudencia relacionada.

Con el propósito de generar coincidencia con los informes previos del Grupo de Expertos Gubernamentales, México reconoce el papel y desarrollos que en la materia pueden tener los organismos regionales, y en particular para la aplicación de medidas de fomento de la confianza. Con base en ello, el Gobierno de México ha estimulado a sus órganos nacionales a considerar el desarrollo de medidas de fomento de la confianza previstas en los informes del Grupo de Expertos Gubernamentales y desarrolladas con más amplitud en los trabajos en la OEA.

El concepto de fortalecimiento de capacidades que emana de los informes del Grupo de Expertos Gubernamentales para México es de capital importancia, pues no solo hace referencia al desarrollo de capacidades nacionales en materia de seguridad de la información sino también a la necesidad de recurrir a todas las modalidades de la cooperación internacional que se ha demostrado que contribuyen a la seguridad y la paz internacionales. El desarrollo de capacidades permite que los Estados y el conjunto de actores interesados estén mejor equipados para hacer frente a las amenazas cibernéticas y fomenta el entendimiento común sobre los distintos temas relacionados con la ciberseguridad.

El Gobierno de México en el periodo que se informa ha buscado también por ello favorecer las sinergias entre los distintos grupos, foros, órganos e iniciativas del sistema de Naciones Unidas que abordan temas relacionados con las tecnologías de la información, las telecomunicaciones, la ciberseguridad, la gobernanza del ciberespacio, la cooperación digital y el cambio tecnológico con el propósito de lograr una mayor coherencia, evitar la duplicación de esfuerzos y aprovechar mejor los recursos de la cooperación.

Singapur

[Original: inglés]
[27 de abril de 2020]

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

Singapur participa tanto en el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional como 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. Singapur reitera que considera esas dos plataformas complementarias y que seguirá contribuyendo de manera constructiva a esos procesos. Para que ambos procesos tengan éxito, su labor debe llevarse a cabo en un espíritu de cooperación constructiva, consenso, respeto mutuo y confianza mutua. En su calidad de copresidente, junto con Estonia, del Grupo de Amigos sobre Gobernanza Electrónica y Ciberseguridad, Singapur se ha comprometido a hacer que

todos los países apoyen la labor de esos dos procesos. Singapur considera que la reunión consultiva oficiosa entre períodos de sesiones del Grupo de Trabajo de Composición Abierta, presidida por el Director Ejecutivo de la Agencia de Ciberseguridad de Singapur, David Koh, fue útil para facilitar un intercambio interactivo entre los Estados Miembros, el sector privado, la sociedad civil, los círculos académicos y la comunidad técnica sobre una serie de cuestiones sustantivas.

Singapur considera que los Estados deben promover la sensibilización sobre las normas voluntarias y no vinculantes existentes sobre el comportamiento responsable de los Estados y apoyar su aplicación. Singapur es partidario de que se sigan elaborando ese tipo de normas cuando sea necesario. Por ejemplo, la infraestructura de información crítica supranacional podría considerarse una categoría especial de esa infraestructura crítica, cuya protección es responsabilidad compartida de todos los Estados Miembros, y puede incluirse en el conjunto de normas existentes[11].

Las organizaciones regionales pueden desempeñar un importante papel. La Asociación de Naciones de Asia Sudoriental (ASEAN) reafirmó la necesidad de establecer un orden internacional basado en normas en el ciberespacio en la primera declaración de los dirigentes de la ASEAN sobre la cooperación en materia de ciberseguridad, publicada en abril de 2018. En septiembre de 2018, los participantes de la Tercera Conferencia Ministerial de la ASEAN sobre Ciberseguridad acordaron suscribir en principio las 11 normas del informe de 2015 del Grupo de Expertos Gubernamentales, y centrarse en el fomento de la capacidad regional para aplicar esas normas. En octubre de 2019, la Cuarta Conferencia Ministerial de la ASEAN sobre Ciberseguridad decidió establecer un comité de trabajo para examinar la elaboración de un plan de acción regional a largo plazo para garantizar la aplicación efectiva y práctica de las normas, en particular en las esferas de la cooperación entre los equipos informáticos de respuesta de emergencia, la protección de la infraestructura de información crítica y la asistencia mutua en materia de ciberseguridad.

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 responsable de los Estados. Como parte de este esfuerzo, Singapur estableció en 2016 un programa de capacidad cibernética de la ASEAN de 10 millones de dólares de Singapur para apoyar la creación de capacidad en la ASEAN en materia de políticas, estrategias y cuestiones técnicas relacionadas con la cibernética. Hasta la fecha, 170 funcionarios de los Estados miembros de la ASEAN han recibido capacitación en el marco del programa. Como extensión del Programa de Fomento de la Capacidad Cibernética de los Miembros de la ASEAN, Singapur puso en marcha en octubre de 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 apoyar la formulación de políticas, el desarrollo de estrategias y la capacidad técnica y operacional en materia de ciberseguridad de los países de la ASEAN y estrechar la colaboración con los asociados internacionales.

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

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

marcha varios cursos de capacitación en materia de ciberseguridad en el marco del Programa de Cooperación de Singapur. Seguimos comprometidos a compartir nuestra experiencia y conocimientos con los Estados Miembros de las Naciones Unidas, especialmente con los países pequeños y en desarrollo.

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

a) *Construir una infraestructura resiliente.* La Agencia de Ciberseguridad de Singapur ha elaborado el Plan Maestro de Ciberseguridad de la Tecnología Operacional como parte de los continuos esfuerzos de Singapur por mejorar la seguridad y la resiliencia de sus sectores de infraestructura de información crítica en la prestación de servicios esenciales. El Plan Maestro sirve para mejorar la respuesta intersectorial a la mitigación de las ciberamenazas en el entorno de la tecnología operacional y para fortalecer las asociaciones con la industria y los interesados. En el Plan Maestro de Ciberseguridad de la Tecnología Operacional se presentan iniciativas clave que abarcan las esferas de las personas, los procesos y la tecnología para mejorar las capacidades de los propietarios de nuestra infraestructura de información crítica y de las organizaciones que utilizan sistemas de tecnología operacional.

b) *Crear un ciberespacio más seguro.* Como parte de los esfuerzos por asegurar mejor su ciberespacio y elevar los niveles de ciberhigiene, Singapur introducirá en 2020 el Plan de Etiquetado de Ciberseguridad para los dispositivos inteligentes conectados a la red. El Plan de Etiquetado de Ciberseguridad se pondrá en marcha como un plan voluntario para dar tiempo al mercado y a los desarrolladores para entender qué beneficios pueden obtener. Las etiquetas de ciberseguridad proporcionarán una indicación del nivel de seguridad incorporado en los productos. Los consumidores pueden elegir productos con mejores calificaciones de seguridad utilizando la información de la etiqueta de ciberseguridad. El Plan de Etiquetado de Ciberseguridad tiene por objeto incentivar a los fabricantes a que desarrollen y ofrezcan productos con características de ciberseguridad reconocidas y mejoradas.

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. También existe una creciente necesidad de establecer un grupo de personas con talento que puedan asumir funciones de liderazgo en materia de ciberseguridad en las organizaciones. Desde su creación en 2015, la Agencia de Ciberseguridad ha colaborado con organismos gubernamentales, asociaciones, asociados de la industria e instituciones de enseñanza superior de Singapur para ampliar y desarrollar la fuerza de trabajo en el campo de la ciberseguridad. La Agencia de Ciberseguridad está encabezando una nueva iniciativa nacional de cibertalentos del Gobierno de Singapur para atraer y educar a los entusiastas con talento de la ciberseguridad desde una edad temprana y ayudar a los profesionales de la ciberseguridad a profundizar sus conocimientos. El objetivo de la iniciativa de cibertalentos es llegar al menos a 20.000 personas en tres años.

Turquía

[Original: inglés]
[22 de mayo de 2020]

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

La tecnología de la información y las comunicaciones (TIC) se ha convertido en parte esencial de la sociedad y la economía. Estas tecnologías se utilizan en una amplia red que incluye los sectores público y privado, la infraestructura crítica y las personas, y se han difundido en Turquía y en el mundo. Como resultado de ello, las TIC desempeñan un papel importante 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.

Turquía centra su labor en la adopción de las medidas necesarias para mejorar la ciberseguridad nacional. El Ministerio de Transporte e Infraestructura es el organismo responsable de formular políticas y elaborar estrategias y planes de acción de ciberseguridad nacional en Turquía. En este contexto, la estrategia y el plan de acción nacionales de ciberseguridad se elaboraron con la participación de todas las partes interesadas en grupos de estudio, bajo la coordinación del Ministerio de Transporte e Infraestructura. Se publicaron y aplicaron la estrategia nacional de ciberseguridad, el plan de acción 2013-2014 y la estrategia y el plan de acción nacionales de ciberseguridad 2016-2019. Turquía ha estado elaborando su próxima estrategia y plan de acción nacionales de ciberseguridad, que se prevé que abarquen los años 2020-2023, y que se publicarán en breve.

Los principales objetivos estratégicos de la próxima estrategia y plan de acción nacionales de ciberseguridad de Turquía son:

- Protección de infraestructuras críticas y aumento de la resiliencia
- Desarrollo de la capacidad
- Seguridad de las nuevas tecnologías (Internet de las cosas, 5G, computación en la nube, etc.)
- Lucha contra la ciberdelincuencia
- Desarrollo y fomento de las tecnologías nacionales
- Red de ciberseguridad orgánica
- Mejora de la cooperación internacional.

Además, el Equipo Nacional de Respuesta a Emergencias Cibernéticas de Turquía, que forma parte de la Autoridad de Tecnologías de la Información y las Comunicaciones, ha coordinado la respuesta a incidentes cibernéticos en Turquía desde 2013. Además de la detección de ciberamenazas y la respuesta a ciberincidentes, antes, durante y después de los incidentes, el Equipo Nacional de Respuesta a Emergencias Cibernéticas se encarga de aplicar medidas preventivas contra las ciberamenazas y asegura la disuasión cibernética. Sus principales áreas de interés en materia de ciberseguridad son: la creación de capacidad cibernética, las medidas tecnológicas, la recopilación y el intercambio de información sobre las amenazas y la protección de la infraestructura crítica.

En el contexto de la mejora de la ciberseguridad nacional, desde 2013 se han establecido también 14 equipos sectoriales de respuesta a emergencias cibernéticas para sectores o infraestructuras críticos (como la energía, la salud, la banca y las finanzas, la gestión del agua, las comunicaciones electrónicas y los servicios públicos críticos) y 1.299 equipos institucionales de respuesta a emergencias cibernéticas. Todos ellos operan de manera ininterrumpida bajo la coordinación del equipo nacional con el fin de mitigar los riesgos cibernéticos y luchar contra las ciberamenazas.

El Equipo Nacional de Respuesta a Emergencias Cibernéticas organiza y apoya cursos de capacitación, campamentos de verano y concursos sobre ciberseguridad abiertos a varias comunidades. Además, imparte cursos de capacitación para los equipos de respuesta a emergencias cibernéticas en materia de análisis de programas maliciosos y análisis de registros, entre otras esferas. El Equipo Nacional de Respuesta a Emergencias Cibernéticas ha capacitado a más de 4.500 personas en diferentes áreas de la ciberseguridad en los últimos tres años.

Los estudios sobre medidas tecnológicas incluyen la detección temprana, las alarmas y las actividades de alerta. Para ello, Turquía ha desarrollado sistemas de detección y prevención. Estos sistemas desempeñan un papel fundamental en el aumento del nivel de ciberseguridad en Turquía.

Varias organizaciones, instituciones, universidades, organizaciones no gubernamentales y el sector privado de Turquía también organizan seminarios, conferencias y cursos de capacitación en todo el país sobre ciberseguridad, protección de infraestructuras críticas y otros temas conexos.

Además, todos los años se organiza un Día de Internet Seguro para realizar actividades de sensibilización sobre el uso consciente y seguro de Internet. Se han puesto en marcha una línea de ayuda por Internet y un sitio web seguro, donde las familias pueden encontrar consejos para el uso eficiente de Internet (https://www.guvenlinet.org.tr/).

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. La privacidad y la protección de los datos personales es también una de las principales preocupaciones en materia de seguridad. En este sentido, en 2016 entró en vigor la Ley núm. 6698 de protección de datos personales para proteger la privacidad.

Turquía ha desempeñado un papel importante en muchas organizaciones, ya sea como miembro fundador o contribuyendo a los esfuerzos de cooperación en materia de ciberseguridad y seguridad de la información. En este contexto, Turquía considera importante el intercambio de información con diferentes países y organizaciones en una amplia gama de esferas. El Equipo Nacional de Respuesta a Emergencias Cibernéticas de Turquía es miembro del Foro de Equipos de Seguridad y Respuesta a Incidentes, el servicio Trusted Introducer, la Unión Internacional de Telecomunicaciones (UIT), la Plataforma Multinacional de Intercambio de Información sobre Programas Maliciosos de la Organización del Tratado del Atlántico Norte (OTAN) y la Alianza de Ciberseguridad para el Progreso Mutuo. Turquía también ha participado en el Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN en calidad de país patrocinador desde noviembre de 2015. Además, existe una cooperación bilateral y multilateral en materia de ciberseguridad, como los memorandos de entendimiento con muchos países. Asimismo, Turquía participa y contribuye activamente a los estudios de organizaciones internacionales como la OTAN, las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa, la Organización de Cooperación y Desarrollo Económicos, el Grupo de los

20, el Consejo de Cooperación de los Estados de Habla Túrquica y el Centro de Cooperación en materia de Seguridad del RACVIAC.

Los ejercicios de ciberseguridad son otra actividad importante para la cooperación y la preparación. Este tipo de ejercicios realizados en los planos nacional e internacional contribuyen a fortalecer el ciberespacio y a poner a prueba las medidas que deben adoptarse contra posibles ciberamenazas. Desde 2011, el Ministerio de Transporte e Infraestructura ha organizado cuatro ejercicios de seguridad cibernética nacionales y dos internacionales. Más recientemente, el 19 de diciembre de 2019, el Ministerio de Transporte e Infraestructura y la Autoridad de las Tecnologías de la Información y las Comunicaciones organizaron conjuntamente en Ankara (Turquía) el ejercicio de seguridad cibernética internacional Cyber Shield 2019, que recibió el apoyo de la UIT y la Alianza de Seguridad Cibernética para el Progreso Mutuo. Además, Turquía participa en ejercicios internacionales de ciberseguridad y contribuye a su realización, como el ejercicio Locked Shields (Escudos Bloqueados) de la OTAN, la Coalición Cibernética de la OTAN y el Ejercicio de Gestión de Crisis de la OTAN.

Turquía ha ratificado también el Convenio sobre la Ciberdelincuencia, que abarca diversos delitos, como los cometidos a través de 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.

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

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

La necesidad de orientación sobre la seguridad de las tecnologías de nueva generación (Internet de las cosas, 5G, computación en la nube, etc.) es otro punto que debe tenerse en cuenta. Las guías o recomendaciones de seguridad de referencia para las tecnologías de nueva generación, que se preparan con la cooperación de los Estados Miembros, contribuirán a aumentar los niveles de preparación para las nuevas ciberamenazas que las acompañan. Además, al igual que los demás estudios de creación de capacidad y orientación, los ejercicios internacionales de ciberseguridad siguen siendo esenciales para aumentar los niveles de preparación y crear capacidad de respuesta a los ciberincidentes en todo el mundo.

Ucrania

[Original: inglés]
[29 de mayo de 2020]

Desde el comienzo de la agresión híbrida de la Federación de Rusia contra Ucrania, han surgido nuevas amenazas y desafíos, entre los que la utilización de mecanismos de influencia cibernética en detrimento de la seguridad del Estado de Ucrania ha ocupado un lugar importante.

Ucrania se mantiene firme en su compromiso con el derecho internacional sobre el uso de la tecnología de la información y las comunicaciones (TIC), así como con su pleno apoyo a las conclusiones y recomendaciones que figuran en los informes del Grupo de Expertos Gubernamentales. En primer lugar, se refiere a la preservación de

la igualdad soberana de los Estados, el no uso o amenaza de uso de la fuerza contra la integridad territorial de los Estados, la no injerencia en los asuntos internos de otros Estados y el respeto de los derechos humanos y las libertades fundamentales.

A fin de organizar una acción eficaz para contrarrestar las amenazas en el ciberespacio y la reglamentación jurídica del comportamiento en el ciberespacio, y esbozando al mismo tiempo el desarrollo del sistema de medidas para contrarrestar esas amenazas a nivel estatal, se aprobaron una serie de reglamentos, entre los que destaca la Estrategia de Ciberseguridad de Ucrania aprobada por el Consejo Nacional de Seguridad y Defensa, la decisión sobre la estrategia de ciberseguridad de Ucrania (promulgada por el Decreto núm. 96 del Presidente de Ucrania, de 15 de marzo de 2016) y la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania, de 5 de mayo de 2017.

Otro mecanismo para contrarrestar las ciberamenazas fue el uso de las disposiciones de la Ley de Ucrania sobre sanciones, de 14 de agosto de 2014, que permitió organizar una respuesta rápida a las amenazas detectadas mediante la aplicación de medidas restrictivas contra una serie de personas jurídicas y físicas que participaban en medidas destinadas a menoscabar la seguridad nacional de Ucrania.

En la actualidad, la protección cibernética de los recursos de información electrónica del Estado y la infraestructura crítica de Ucrania se lleva a cabo de conformidad con la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania. Las definiciones de la autoridad, las tareas y las funciones de los sujetos de la ciberseguridad consagradas en esta Ley sirven para establecer un sistema holístico de ciberseguridad.

A este respecto, el principio básico del desarrollo de la política pública en el ámbito de la ciberseguridad y la ciberdefensa es la elaboración de un marco regulatorio compatible con los enfoques y normas internacionales. Para llevar a cabo esta tarea, se han adoptado las siguientes medidas:

- Se aprobó la Resolución del Gobierno de Ucrania sobre la aprobación de los requisitos generales para la protección cibernética de la infraestructura crítica. Los enfoques de la ciberseguridad definidos en esta resolución tienen en cuenta los requisitos de las normas internacionales en materia de seguridad de la información y aplican las directivas de la Unión Europea, lo que hace que el Estado participe en pie de igualdad en el espacio de seguridad mundial.
- Se han elaborado proyectos de resolución del Gobierno de Ucrania:
  - Sobre la aprobación del procedimiento de examen del estado de la protección cibernética de la infraestructura de información crítica, los recursos de información y la información del Estado, cuyo requisito de protección está establecido por ley
  - Sobre la aprobación del procedimiento para la designación de instalaciones de infraestructura crítica
  - Sobre la aprobación del procedimiento de elaboración de una lista de instalaciones de infraestructura de información crítica, la inclusión de las instalaciones de infraestructura de información crítica en el registro estatal de instalaciones de infraestructura de información crítica, y su formación y funcionamiento, teniendo en cuenta los requisitos de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

– Sobre la aprobación del protocolo sobre acciones conjuntas de las entidades de ciberseguridad y los propietarios (administradores) de instalaciones de infraestructura de información crítica durante la detección, prevención e interrupción de ciberataques y ciberincidentes, así como durante la eliminación de sus consecuencias.

A fin de mejorar el sistema de protección técnica y criptográfica de la información, se introdujo la hoja de ruta para reformar el ámbito de la protección de la información adaptando la legislación de Ucrania a los requisitos de la legislación de la Unión Europea. Para aplicar esta hoja de ruta se ha elaborado un proyecto de ley sobre la seguridad de la información y los sistemas de comunicación e información.

Uno de los elementos clave para el desarrollo eficaz del sistema nacional de ciberseguridad es el examen del estado de la ciberseguridad. Los resultados del examen servirán de base para elaborar una nueva estrategia nacional de ciberseguridad o ajustar la estrategia existente, mejorar el marco regulatorio de las entidades de ciberseguridad, financiar medidas de protección cibernética de los recursos de información y la infraestructura crítica del Estado, mejorar el sistema de capacitación de recursos humanos en materia de ciberseguridad, elaborar nuevos enfoques para el fomento de la cooperación entre los sectores público y privado en esta esfera, y fortalecer el intercambio de información entre los sujetos de la ciberseguridad y su interacción al abordar las cuestiones de seguridad.

Además, a fin de reforzar la seguridad de la información y promover la cooperación internacional en esta esfera, el Servicio Estatal de Comunicaciones Especiales ha adoptado medidas para:

- El funcionamiento del Equipo Informático de Respuesta de Emergencia de Ucrania, que está acreditado por el Foro de Equipos de Respuesta a Incidentes Cibernéticos e interactúa con otros equipos de 96 Estados
- El control estatal sobre el estado de la protección en el ciberespacio y la protección técnica de los recursos de información y la información del Estado, cuyo requisito de protección está establecido por ley
- La participación en las reuniones de los puntos de contacto nacionales utilizando la Red de Comunicaciones de la Organización para la Seguridad y la Cooperación en Europa (OSCE)
- La sensibilización pública y la realización de seminarios prácticos sobre ciberseguridad para los sujetos del sistema nacional de ciberseguridad
- La interacción con los organismos encargados de hacer cumplir la ley y la información oportuna sobre los ciberataques
- La coordinación, organización y realización de una auditoría de los sistemas de comunicación y tecnológicos de las instalaciones de infraestructura crítica, realizando la auditoría de la seguridad de la información de conformidad con la Norma Estatal de Ucrania ISO/IEC 27001: 2015.

Habida cuenta de los desafíos y amenazas actuales, se están estableciendo mecanismos jurídicos en la esfera de la ciberdefensa en Ucrania con miras a:

- Aumentar la seguridad de las redes y los sistemas de información, cuyo principal objetivo debería ser la protección eficaz de la información y los datos, garantizando la estabilidad de las redes y los sistemas y la continuidad de sus funciones, así como la eficacia de la detección, la respuesta y la reducción al mínimo de la recuperación después de incidentes cibernéticos
- Aplicar un sistema de gestión de riesgos

- Crear condiciones para el suministro de recursos, incluidos los recursos humanos, en la esfera de la ciberseguridad
- Fortalecer la resiliencia operacional y cibernética y de las instalaciones de infraestructura crítica
- Establecer un sistema para conservar los recursos de información del Estado y garantizar la protección de la información tecnológica, que es fundamental para el funcionamiento de las instalaciones de infraestructura crítica
- Participar en el Comité de Criterios Comunes mediante la adhesión al acuerdo pertinente (Acuerdo sobre el Reconocimiento de Certificados de Criterios Comunes en la esfera de la Seguridad de la Tecnología de la Información), que garantizará la inclusión de los productos certificados en Ucrania en el registro reconocido por los países de la Unión Europea y otros países líderes en ese ámbito
- Asegurar el estricto cumplimiento de los requisitos de la legislación en materia de protección de los recursos de información del Estado y la protección criptográfica y técnica de la información, incluida la protección de los datos personales, por parte de los jefes de los órganos que gestionan las instalaciones de infraestructura de información crítica
- Aprovechar las oportunidades de colaboración entre los sectores público y privado y de interacción entre las partes interesadas para solucionar los problemas de ciberdefensa y ciberseguridad
- Elevar el nivel de la cultura del comportamiento en Internet
- Participar de manera activa en las iniciativas pertinentes de la comunidad internacional y unirse a las estructuras correspondientes de las principales organizaciones internacionales.

De 2015 a 2020, el Consejo Nacional de Seguridad y Defensa de Ucrania adoptó decisiones anuales sobre la aplicación de medidas económicas especiales personales y otras medidas restrictivas (sanciones), que se aplicaron mediante los decretos pertinentes del Presidente de Ucrania.

Además de lo anterior, el Servicio de Seguridad de Ucrania, como una de las principales entidades responsables de la ciberseguridad, de conformidad con su competencia definida por la ley, está adoptando medidas para mejorar el marco regulatorio nacional sobre el ciberespacio. En particular, se trabaja de manera continua para determinar las normas necesarias para la aplicación de la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania.

Se están adoptando medidas para aplicar las disposiciones de la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania al marco regulatorio que rige las actividades del Servicio de Seguridad de Ucrania.

Sin embargo, a pesar de esas medidas, la cuestión de la mejora del marco regulatorio en la esfera de la información y la ciberseguridad sigue siendo pertinente hoy en día.

En particular, varias iniciativas legislativas relativas al Servicio de Seguridad, que estaban siendo examinadas por los comités de la Rada Suprema de Ucrania de la anterior asamblea, aún no han sido examinadas por los parlamentarios ucranianos (fortalecimiento de la responsabilidad penal por los delitos cibernéticos, división de los poderes de investigación entre el Servicio de Seguridad y la Policía Nacional, y establecimiento de la responsabilidad por incumplimiento).

Las disposiciones del Convenio sobre la Ciberdelincuencia no se han aplicado plenamente.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, de 23 de noviembre de 2001, fue ratificado por la Rada Suprema en septiembre de 2005. Las disposiciones del Convenio abarcan la responsabilidad penal por los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, a saber: acceso ilegal, interceptación ilegal, interferencia de datos, interferencia de sistemas y uso indebido de dispositivos. Es decir, esas disposiciones del Convenio abarcan los delitos contra el funcionamiento sostenible de la infraestructura crítica.

Sin embargo, varias disposiciones del Convenio sobre la Ciberdelincuencia no se aplican actualmente en la legislación nacional, lo que limita las actividades de los organismos encargados de hacer cumplir la ley para detectar y prevenir la ciberdelincuencia. En particular, las disposiciones del Convenio sobre la Ciberdelincuencia que deben aplicarse se refieren a la conservación rápida de datos informáticos almacenados, la conservación y revelación parcial rápidas de datos sobre el tráfico, el procedimiento para una orden de presentación, el registro y confiscación de datos informáticos almacenados y la obtención en tiempo real de datos de tráfico (artículos 16 a 20). También es necesario enmendar el Código de Procedimiento Penal de Ucrania para introducir una categoría independiente de pruebas, a saber, las pruebas digitales en los procedimientos penales.

En la actualidad, los representantes del Servicio de Seguridad de Ucrania en el grupo de trabajo del Comité sobre Cumplimiento de la Ley de la Rada Suprema están trabajando en el proyecto de ley de Ucrania para enmendar determinados actos legislativos relativos a la aplicación del Convenio sobre la Ciberdelincuencia con el fin de normalizar las disposiciones del Convenio en la legislación de Ucrania, mejorar las disposiciones del Código de Procedimiento Penal de Ucrania y establecer un mecanismo jurídico eficaz para luchar contra la ciberdelincuencia, entre otras cosas:

- Otorgando a los jefes de la unidad operacional, al investigador y al fiscal la facultad de dar instrucciones obligatorias a los propietarios de datos informáticos (operadores y proveedores de telecomunicaciones, y otras personas jurídicas y físicas) para la conservación rápida de los datos informáticos necesarios para resolver el delito, por un período de hasta 90 días
- Estableciendo requisitos para la divulgación por parte de los operadores y proveedores de telecomunicaciones, a petición de los organismos encargados de hacer cumplir la ley, de la información necesaria para identificar a los proveedores de servicios y descubrir la ruta por la que se transmitió la información
- Estableciendo un mecanismo eficaz para el uso de pruebas en forma electrónica (digital) en los procedimientos penales
- Introduciendo enmiendas al Código de Procedimiento Penal de Ucrania, la Ley de telecomunicaciones y el proyecto de ley sobre comunicaciones electrónicas a fin de garantizar el establecimiento de un mecanismo jurídico para restringir temporalmente el acceso a la información o los datos informáticos publicados en un determinado recurso (servicio) de información (identificado) y determinar el procedimiento para su aplicación.

El 4 de febrero de 2020 la Rada Suprema retiró el proyecto de ley sobre comunicaciones electrónicas (Reg. núm. 2264), sobre el que el Servicio de Seguridad de Ucrania había presentado observaciones y propuestas por conducto del Comité sobre Transformación Digital de la Rada Suprema a finales de 2019.

El 5 de febrero de 2020 se registró en la Rada Suprema un proyecto de ley, núm. 3014, con el mismo título (sobre comunicaciones electrónicas) y un equipo de autores casi idéntico. Según un análisis preliminar, el nuevo proyecto de ley tampoco contiene disposiciones que faciliten la plena aplicación de las disposiciones del Convenio sobre la Ciberdelincuencia.

Para abordar las cuestiones actuales en el ámbito de la ciberseguridad en 2020, el Servicio de Seguridad de Ucrania apoyó la introducción de una iniciativa legislativa para el examen de varios proyectos de ley por la Rada Suprema de la novena asamblea. La aprobación de los proyectos de ley establecerá una base jurídica para el Servicio de Seguridad de conformidad con la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania.

En particular, existe una distinción legislativa entre los investigadores de la Policía Nacional y las autoridades de seguridad para la investigación de los delitos cometidos con el uso de computadoras, sistemas y redes informáticas y de telecomunicaciones, recursos de información del Estado e infraestructura de información crítica, y se refuerzan las penas por la comisión de estos delitos.

La ejecución de las tareas relacionadas con la prevención, detección, interrupción y divulgación de los delitos contra la paz y la seguridad de la humanidad cometidos en el ciberespacio y la aplicación de medidas de contrainteligencia e investigación destinadas a combatir el ciberterrorismo y el ciberespionaje requieren la introducción de enmiendas en la Ley de contrainteligencia para complementar las funciones y facultades de los órganos, subdivisiones y empleados del Servicio de Seguridad de Ucrania.

Además, no se han establecido a nivel legislativo los principios y directrices para la construcción del sistema estatal de protección de infraestructura crítica, ni se ha definido la infraestructura crítica del Estado a nivel de reglamentos (no se ha establecido aún la Lista de Objetos de Infraestructura Crítica ni la Lista de Objetos de Infraestructura de Información Crítica).

En 2019, el Gobierno aprobó los Requisitos Generales para la Protección Cibernética de las Instalaciones de Infraestructura Crítica (Resolución núm. 518 del Consejo de Ministros de Ucrania, de 19 de junio de 2019). Este acto jurídico no es válido si no se dispone de la Lista Estatal de Infraestructura Crítica y de la Lista de Infraestructura de Información Crítica, cuya existencia está prevista en la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania.

La incertidumbre en cuanto a la infraestructura crítica del Estado complica la ejecución de la ciberseguridad y de las tareas de ciberseguridad asignadas al Servicio de Seguridad de Ucrania y a otros agentes de ciberseguridad.

La necesidad de asegurar la elaboración y aprobación de la Ley sobre la infraestructura crítica y su protección, así como de acelerar la aprobación de las medidas del Consejo de Ministros de Ucrania encaminadas a aplicar las disposiciones de la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania fue puesta de relieve por el Comité sobre Transformación Digital de la Rada Suprema en una reunión sobre la ciberseguridad nacional y la ciberdefensa de Ucrania, en particular en la esfera de la infraestructura crítica, que se celebró el 23 de diciembre de 2019.

La cuestión de la aplicación práctica de la Ley sobre los principios básicos del mantenimiento de la ciberseguridad de Ucrania y la adopción de los reglamentos necesarios para su aplicación se examinó por separado en una reunión del Comité sobre Transformación Digital de la Rada Suprema, que se celebró el 19 de febrero de 2020.

Sigue siendo pertinente el problema de la falta de reglamentación para reducir la dependencia crítica por parte de las instituciones, organizaciones y empresas nacionales del *software* extranjero, que puede contener vulnerabilidades aplicadas intencionalmente y funciones no documentadas.

Según los especialistas del Servicio de Seguridad de Ucrania, esto requiere la elaboración de un programa nacional de sustitución de importaciones en la esfera de la informatización, un conjunto de medidas de apoyo a los productores nacionales de *software* y la creación de:

- Un registro de proveedores de *software* verificados para instalaciones de infraestructura de información crítica, y la preparación del procedimiento para su inclusión o exclusión del registro específico
- Un registro de *software* privativo cuyo uso se recomienda en instalaciones de infraestructura de información crítica
- Un depósito nacional de *software* gratuito y una mayor aplicación de los programas estatales para transferir su uso a las autoridades públicas y la administración.

Además, a fin de establecer un procedimiento legislativo para dar una respuesta inmediata y eficaz a las amenazas existentes y potenciales a los intereses nacionales y a la seguridad de Ucrania en la esfera de la tecnología de la información y las comunicaciones, es necesario introducir las modificaciones pertinentes en la Ley de sanciones: la introducción de restricciones al uso por parte de la infraestructura crítica de todas las formas de propiedad de *software* (incluidos los antivirus) y equipos de telecomunicaciones que hayan sido desarrollados o fabricados por entidades económicas del país agresor.

Otro factor que tiene repercusiones negativas son las lagunas de la legislación interna en lo que respecta a la falta de un mecanismo legalmente definido para bloquear el acceso de un usuario a los recursos de Internet y eliminar los mensajes que contienen información obtenida ilegalmente.

Cabe señalar también que el Servicio de Seguridad de Ucrania aplica medidas de cooperación internacional en la esfera del fortalecimiento de la información y la ciberseguridad. Las principales prioridades y esferas, según la estrategia de ciberseguridad de Ucrania, son las siguientes:

- El desarrollo de la cooperación internacional en el ámbito de la ciberseguridad
- El apoyo a las iniciativas internacionales en materia de ciberseguridad que respondan a los intereses nacionales de Ucrania
- La intensificación de la cooperación de Ucrania con la Unión Europea y la Organización del Tratado del Atlántico Norte (OTAN) para fortalecer la capacidad de Ucrania en materia de ciberseguridad
- La participación en medidas de fomento de la confianza en el ciberespacio bajo los auspicios de la OSCE.

En particular, el Servicio de Seguridad de Ucrania, dentro de sus esferas de competencia, participa en las actividades de CyberEast, un proyecto conjunto de la Unión Europea y el Consejo de Europa para los países del programa de la Asociación Oriental, que tiene por objeto aplicar decisiones legislativas y de política para poner en práctica las disposiciones del Convenio sobre la Ciberdelincuencia de Budapest. El proyecto CyberEast es ejecutado por la Dirección General de Política de Vecindad y Negociaciones de Ampliación de la Unión Europea, junto con la Oficina del Programa de Ciberdelincuencia del Consejo de Europa.

Habida cuenta de la importancia de informar a los asociados internacionales sobre los últimos logros de Ucrania en materia de ciberseguridad, y de la aplicación de determinadas medidas de fomento de la confianza de conformidad con las decisiones núms. 1039, 1106 y 1202 del Consejo Permanente de la OSCE en el ámbito de las TIC y del uso de las TIC, los representantes del Servicio de Seguridad de Ucrania suelen participar en las reuniones del Grupo de Trabajo Oficioso de la OSCE sobre las TIC. Además, el Servicio de Seguridad de Ucrania ha establecido un punto de contacto en el marco de la medida de fomento de la confianza núm. 8 establecida en la decisión 1202, que realiza actividades a nivel profesional como parte de los controles de comunicación planificados y no planificados.

El Servicio de Seguridad de Ucrania también participa en un proyecto de la OSCE, cuyo principal objetivo es realizar un análisis detallado de la estructura de gobernanza nacional en el ámbito de la ciberseguridad y aplicar las medidas de fomento de la confianza de Ucrania en el ámbito de las TIC y la ciberseguridad, como se establece en la Decisión 1202.

Además, de conformidad con las tareas asignadas al Servicio de Seguridad de Ucrania, con el apoyo del Fondo Fiduciario de la OTAN para la Ciberseguridad de Ucrania, se obtuvo el equipo necesario y se creó el Centro de Situación para la Ciberseguridad del Servicio de Seguridad de Ucrania, con miras a:

- Prevenir, detectar y eliminar los crímenes contra la paz y la seguridad de la humanidad cometidos en el ciberespacio
- Establecer medidas de contrainteligencia e investigación destinadas a combatir el ciberterrorismo y el ciberespionaje
- Verificar la preparación de las instalaciones de infraestructura crítica para responder a posibles ciberataques y ciberincidentes
- Contrarrestar la ciberdelincuencia, cuyas consecuencias pueden amenazar los intereses esenciales del Estado
- Investigar ciberincidentes y ciberataques contra los recursos de información electrónica y la infraestructura de información crítica del Estado
- Garantizar la respuesta a los ciberincidentes en el ámbito de la seguridad del Estado.

El Servicio de Seguridad de Ucrania también ha iniciado la cooperación en materia de intercambio de información sobre ciberamenazas, ciberataques y ciberincidentes utilizando la plataforma de intercambio de información sobre programas informáticos maliciosos e intercambio de amenazas Ukrainian Advantage. Se trata de una plataforma pública de cooperación entre el Servicio de Seguridad de Ucrania y las instalaciones de infraestructura crítica, otras empresas, instituciones y organizaciones, independientemente de su titularidad, y también personas, cuyo objetivo es mejorar la seguridad de los usuarios de la información, las telecomunicaciones y los sistemas de información y telecomunicaciones para los cuales están autorizados a brindar protección en virtud de los acuerdos pertinentes u otros fundamentos jurídicos.

III. Respuestas recibidas de organizaciones intergubernamentales

Unión Europea

[Original: inglés]
[20 de mayo de 2020]

El ciberespacio, y en particular la Internet global y abierta, se ha convertido en uno de los ejes principales de nuestras sociedades. Ofrece una plataforma que impulsa la conectividad y el crecimiento económico. La Unión Europea y sus Estados miembros apoyan un ciberespacio mundial, abierto, estable, pacífico y seguro en el que se apliquen plenamente los derechos humanos y las libertades fundamentales y el estado de derecho, con miras a lograr el bienestar de la sociedad, el crecimiento económico, la prosperidad, y la integridad de las sociedades libres y democráticas.

A medida que Internet penetra cada vez más en nuestras vidas, muchos de los problemas que enfrentamos en el mundo físico surgen también en el ciberespacio. En el contexto internacional, algunos Estados parecen haber adoptado una visión del ciberespacio que entraña un alto grado de control gubernamental, lo que suscita preocupaciones relacionadas con las violaciones de los derechos humanos y las libertades fundamentales. También se ha producido un alarmante aumento de las actividades cibernéticas malintencionadas de agentes estatales y no estatales. La Unión Europea y sus Estados miembros han expresado periódicamente su preocupación por esas actividades malintencionadas, que socavan el orden internacional basado en normas y aumentan los riesgos de conflicto.

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

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

La estrategia de ciberseguridad “Un ciberespacio abierto, protegido y seguro”[12], así como otros documentos de política posteriores que se citan a continuación, representan la visión global de la Unión Europea sobre la mejor manera de prevenir y responder a las perturbaciones y los ataques cibernéticos. Su objetivo es promover los valores de la Unión Europea y asegurar que se den las condiciones para que la

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

economía digital crezca. Algunas medidas específicas están destinadas a aumentar la ciberresiliencia de los sistemas de información, reducir la ciberdelincuencia y fortalecer la política internacional de ciberseguridad y ciberdefensa de la Unión Europea.

En febrero de 2015, el Consejo de la Unión Europea subrayó en sus Conclusiones del Consejo sobre la Ciberdiplomacia[13] la importancia de seguir desarrollando y ejecutando un planteamiento común y global de la Unión Europea para la ciberdiplomacia que promueva los derechos humanos y los valores fundamentales de la Unión Europea, garantice la libertad de expresión, fomente la igualdad de género, impulse el crecimiento económico, luche contra la ciberdelincuencia, contrarreste las amenazas para la ciberseguridad, evite los conflictos y proporcione estabilidad en las relaciones internacionales. La Unión Europea también pide que se refuerce el modelo multisectorial de gobernanza de Internet y que se intensifiquen los esfuerzos de creación de capacidad en terceros países. Además, la Unión Europea reconoce la importancia de colaborar con los principales asociados y las organizaciones internacionales. La Unión Europea también hace hincapié en la aplicación del derecho internacional vigente en el ámbito de la seguridad internacional y en la pertinencia de las normas de comportamiento, así como en la importancia de la gobernanza de Internet como parte integrante del enfoque común y global de la Unión Europea en materia de ciberdiplomacia.

Sobre la base de un examen de la Estrategia de Ciberseguridad de 2013, la Unión Europea siguió reforzando sus estructuras y capacidades en materia de ciberseguridad de manera coordinada, con la plena cooperación de los Estados miembros y las distintas estructuras de la Unión Europea pertinentes, respetando al mismo tiempo sus competencias y responsabilidades. En la comunicación conjunta de 2017 titulada "Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE[14]" se establecieron la magnitud del reto y la gama de medidas previstas en la Unión Europea, para garantizar que esté mejor preparada para hacer frente a los crecientes desafíos cada vez mayores de la ciberseguridad.

La preocupación por los crecientes problemas de ciberseguridad impulsó la elaboración de un marco para una respuesta diplomática conjunta de la Unión Europea a las actividades informáticas malintencionadas, el conjunto de instrumentos de ciberdiplomacia[15]. La capacidad y disposición crecientes de agentes estatales y no estatales de perseguir sus objetivos mediante actividades cibernéticas malintencionadas debería ser motivo de preocupación a nivel mundial. Esas actividades pueden constituir actos ilegales con arreglo al derecho internacional y podrían tener efectos desestabilizadores y en cascada con mayores riesgos de conflicto. La Unión Europea y sus Estados miembros están firmemente decididos a solucionar las controversias internacionales en el ciberespacio por medios pacíficos. Con este fin, el marco para una respuesta diplomática conjunta de la Unión Europea forma parte del planteamiento de la Unión Europea en materia de ciberdiplomacia, que contribuye a la prevención de conflictos, a contrarrestar las amenazas para la ciberseguridad y a una mayor estabilidad en las relaciones internacionales. El marco fomenta la cooperación, facilita la lucha contra las amenazas inmediatas y a largo plazo e influye en el comportamiento de los agentes malintencionados a largo plazo. También proporciona la debida coordinación con los mecanismos de gestión de crisis de la Unión Europea, incluido el Plan director de respuesta coordinada a los incidentes

[13] 6122/15 Conclusiones del Consejo sobre la Ciberdiplomacia.

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

[15] 10474/17 Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas ("conjunto de instrumentos de ciberdiplomacia").

y crisis de ciberseguridad a gran escala. La Unión Europea y sus Estados miembros piden a la comunidad internacional que refuerce la cooperación internacional en favor de un ciberespacio mundial, abierto, estable, pacífico y seguro en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el estado de derecho. La Unión Europea está decidida a proseguir sus esfuerzos por prevenir, desalentar, disuadir y responder a las actividades malintencionadas, y trata de mejorar la cooperación internacional a tal efecto.

La política internacional sobre el ciberespacio de la Unión Europea promueve el respeto de los valores fundamentales de la Unión Europea, define normas para un comportamiento responsable y aboga por la aplicación de las leyes internacionales vigentes en el ciberespacio, al tiempo que ayuda a los países no pertenecientes a la Unión Europea a crear capacidad en materia de ciberseguridad y promueve la cooperación internacional en cuestiones cibernéticas.

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

Amenazas existentes y nuevas amenazas

La Unión Europea y sus Estados miembros reconocen que el ciberespacio ofrece importantes oportunidades para el crecimiento económico, así como para el desarrollo sostenible e inclusivo. No obstante, los recientes acontecimientos en el ciberespacio presentan desafíos en constante evolución.

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

Más recientemente, mientras continúa la pandemia de la enfermedad por coronavirus (COVID-19), la Unión Europea y sus Estados miembros han observado ciberamenazas y actividades cibernéticas maliciosas dirigidas a operadores esenciales de los Estados miembros y sus asociados internacionales, incluso en el sector de la atención de la salud. La Unión Europea y sus Estados miembros condenan este comportamiento malintencionado en el ciberespacio y subrayan su continuo apoyo al aumento de la ciberresiliencia.

Cualquier intento de obstaculizar la capacidad de las infraestructuras críticas es inaceptable y puede poner en peligro la vida de las personas. Todos los agentes deben abstenerse de realizar actividades irresponsables y desestabilizadoras en el ciberespacio. La Unión Europea y sus Estados miembros han pedido a todos los países que ejerzan la debida diligencia y adopten medidas apropiadas contra quienes realicen esas actividades desde su territorio, de conformidad con el derecho internacional y los informes de los Grupos de Expertos Gubernamentales de las Naciones Unidas aprobados por consenso de 2010, 2013 y 2015. La Unión Europea y sus Estados miembros insisten una vez más en que los Estados no deben permitir a sabiendas que su territorio se utilice para cometer hechos internacionalmente ilícitos utilizando las TIC y deben también responder a las solicitudes apropiadas de otro Estado para poner fin a las actividades cibernéticas malintencionadas que emanen de su territorio.

Además, como se reconoció en informes anteriores del Grupo de Expertos Gubernamentales, dado el carácter único de la información y las comunicaciones, el enfoque de la Unión Europea para abordar las cuestiones cibernéticas en el contexto

de la seguridad internacional debe seguir siendo tecnológicamente neutro. Esto es coherente con el concepto y con el reconocimiento por parte de las Naciones Unidas de que el derecho internacional vigente se aplica a nuevas esferas, incluido el uso de tecnologías emergentes.

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

Forma en que el derecho internacional se aplica al uso de las tecnologías de la información y las comunicaciones

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

Un marco de ciberseguridad verdaderamente universal solo puede basarse en el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, el derecho internacional humanitario y el derecho internacional de los derechos humanos. Además, la Unión Europea y sus Estados miembros reiteran la aplicabilidad del derecho internacional vigente a la conducta de los Estados en el ciberespacio, como se reconoce en los informes del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015, y los principios establecidos en los párrafos 28 a) a f) del informe de 2015.

El derecho internacional, incluido el derecho internacional humanitario, que incorpora los principios de precaución, humanidad, necesidad militar, proporcionalidad y distinción, se aplica a la conducta de los Estados en el ciberespacio y es totalmente protector, al establecer límites claros para su legalidad, también en tiempos de conflicto. La Unión Europea subraya su convicción de que el derecho internacional no es cómplice de la conducta, sino que perfila las normas que rigen las operaciones militares para limitar sus efectos y, en particular, para proteger a la población civil.

Además, los derechos humanos y las libertades fundamentales consagrados en los instrumentos internacionales pertinentes deben respetarse y defenderse por igual en línea y fuera de línea. La Unión Europea y sus Estados miembros celebran que el Consejo de Derechos Humanos[16] y la Asamblea General también hayan afirmado estos principios.

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

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

Seguimos apoyando los esfuerzos en curso para promover la aplicación del derecho internacional vigente en el ciberespacio, en particular en lo que respecta al

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

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

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

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

La Unión Europea y sus Estados miembros se guiarán, en su uso de las TIC, por el derecho internacional vigente, así como por el cumplimiento de las normas, reglas y principios voluntarios de comportamiento responsable de los Estados y su aplicación en el ciberespacio, tal como se explica en los sucesivos informes del Grupo de Expertos Gubernamentales de 2010, 2013 y 2015. Creemos que para avanzar de una forma práctica se debería alentar una mayor cooperación y transparencia para compartir las mejores prácticas, en particular sobre la forma en que se aplican las normas existentes del Grupo de Expertos Gubernamentales, mediante iniciativas y marcos conexos, como las organizaciones e instituciones regionales, con miras a facilitar la sensibilización y aplicar eficazmente las normas acordadas sobre el comportamiento responsable de los Estados.

Medidas de fomento de la confianza

La creación de mecanismos eficaces de cooperación e interacción entre los Estados en el ciberespacio es un componente esencial de la prevención de conflictos. Los foros regionales han demostrado ser una plataforma pertinente para crear un espacio para el diálogo y la cooperación entre agentes con preocupaciones e intereses comunes, a fin de abordar eficazmente los problemas desde una perspectiva regional.

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

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

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

capacidad de los Estados de responder eficazmente a las ciberamenazas y recuperarse de ellas.

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

La Unión Europea y sus Estados miembros reconocen que la promoción de una capacidad de protección adecuada y de productos, procesos y servicios digitales más seguros contribuirá a que el ciberespacio sea más seguro y fiable. Reconocemos la responsabilidad de todos los agentes pertinentes de participar en el desarrollo de la capacidad a este respecto y pedimos además una cooperación más estrecha con los principales asociados y organizaciones internacionales para apoyar la creación de capacidad en terceros países.