COMISIÓN MUNDIAL
SOBRE LA ESTABILIDAD DEL CIBERESPACIO

IMPULSAR LA CIBERESTABILIDAD

INFORME FINAL
NOVIEMBRE DE 2019

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

FOMENTO DE LA ESTABILIDAD EN EL CIBERESPACIO EN ARAS DE LA PAZ Y LA PROSPERIDAD

La Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC, por sus siglas en inglés) elaborará propuestas de normas y políticas para mejorar la seguridad y la estabilidad internacionales y servir de guía para un comportamiento estatal y no estatal responsable en el ciberespacio.

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

IMPULSAR LA CIBERESTABILIDAD

INFORME FINAL
NOVIEMBRE DE 2019

The Hague Centre for Strategic Studies

***Centro para Estudios Estratégicos de* La Haya**
Lange Voorhout 1 2514
EA La Haya

info@hcss.nl
www.hcss.nl

EastWest INSTITUTE

Instituto EastWest
Nueva York | Bruselas
Moscú | San Francisco

cyber@eastwest.ngo
www.eastwest.ngo

PRESIDENTES

Michael Chertoff EE. UU.
Latha Reddy India
Marina Kaljurand Estonia *(expresidenta)*

COMISIONADOS

Abdul-Hakeem Ajijola Nigeria
Virgilio Almeida Brasil
Isaac Ben-Israel Israel
Scott Charney EE. UU.
Frédérick Douzet Francia
Anriette Esterhuysen Sudáfrica
Jane Holl Lute EE. UU.
Nigel Inkster Reino Unido
Khoo Boon Hui Singapur
Wolfgang Kleinwächter Alemania
Olaf Kolkman Países Bajos
Lee Xiaodong China
James Lewis EE. UU.
Jeff Moss EE. UU.
Elina Noor Malasia
Joseph S. Nye, Jr. EE. UU.
Christopher Painter EE. UU.
Uri Rosenthal Países Bajos
Ilya Sachkov Rusia
Samir Saran India
Marietje Schaake Países Bajos
Motohiro Tsuchiya Japón
Bill Woodcock EE. UU.
Zhang Li China
Jonathan Zittrain EE. UU.

REPRESENTANTES ESPECIALES Y ASESORES

Carl Bildt Suecia
Vint Cerf EE. UU.
Sorin Ducaru Rumanía
Martha Finnemore EE. UU.

DIRECTORES

Alexander Klimburg Austria
Bruce W. McConnell EE. UU.

PRESIDENTES DE GRUPOS ASESORES DE INVESTIGACIÓN

Sean Kanuck EE. UU.
Koichiro Komiyama Japón
Marília Maciel Brasil
Liis Vihul Estonia
Hugo Zylberberg Francia

SECRETARIADO

The Hague Centre for Strategic Studies

EastWest INSTITUTE

ASOCIADOS

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

PATROCINADORES

Departamento Federal de Asuntos Exteriores de Suiza

GLOBSEC

Ministerio de Asuntos Exteriores de Estonia

Ministerio de Asuntos Internos y Comunicaciones de Japón

COLABORADORES

Comisión de la Unión Africana

Black Hat USA

DEF CON

Delegación de la Unión Europea ante las Naciones Unidas en Ginebra

Foro Global de Especialistas en Ciberseguridad

Google

Municipio de La Haya

Packet Clearing House

Universidad de Tel Aviv

Instituto de las Naciones Unidas de Investigación sobre el Desarme

ÍNDICE DE CONTENIDO

CARTA DE LOS PRESIDENTES

El ciberespacio, uno de los más grandes inventos de la humanidad, ha cambiado las relaciones personales, sociales, comerciales y políticas. Lamentablemente, debido a los ataques que se llevan a cabo en el ciberespacio y a través suyo, es necesario tomar medidas urgentes para asegurar su estabilidad. Este concepto de estabilidad del ciberespacio, al igual que su pariente cercano, la estabilidad internacional, requiere una visión compartida, en la que todas las partes reconozcan que los desacuerdos y los cambios geopolíticos que afecten al ciberespacio deben gestionarse con relativa paz, y que debe garantizarse su estabilidad.

La Comisión Mundial sobre la Estabilidad del Ciberespacio emprendió su labor convencida de que un asunto tradicionalmente reservado a los Estados, como es la paz y la seguridad internacionales, ya no podía abordarse sin involucrar a otras partes interesadas. El ciberespacio es un entorno con múltiples partes interesadas: quienes lo crean y lo gestionan, y quienes responden a los ataques en él y a través de él, pueden ser tanto actores no estatales como funcionarios gubernamentales. Hemos seleccionado a nuestros comisionados para que sean el reflejo de esta característica. Aparte de ex altos funcionarios gubernamentales con experiencia en asuntos de seguridad internacional, entre nuestros miembros figuraban líderes reconocidos de los ámbitos de la gobernanza de Internet, las comunidades de los derechos humanos y el desarrollo, así como la tecnología y la industria. Conjuntamente, nuestros 28 Comisionados de 16 países aportaron una amplia gama de experiencias y puntos de vista, y contaron con la ayuda de los comentarios del público en respuesta a las actividades de divulgación de la Comisión.

El informe final de la Comisión es el resultado de tres años de duro trabajo. Agradecemos sinceramente a quienes lo hicieron posible: nuestros Comisionados, nuestros asesores e investigadores (muchos de ellos también voluntarios), nuestros patrocinadores financieros y nuestra junta directiva. Por último, expresamos nuestro agradecimiento al Secretariado, que no solo ha gestionado eficazmente el proceso, sino que ha contribuido decisivamente a la creación de la Comisión como iniciativa de la sociedad civil.

En el curso de su trabajo, la Comisión se mantuvo al tanto de otras iniciativas sobre el ciberespacio, tanto pasadas como presentes. Nuestro informe, titulado *Impulsar la ciberestabilidad*, complementa y afianza la labor de otros, a la vez que aporta nuevas ideas para impulsar la estabilidad del ciberespacio.

Michael Chertoff
Copresidente
Comisión Mundial sobre la Estabilidad del Ciberespacio

Latha Reddy
Copresidente
Comisión Mundial sobre la Estabilidad del Ciberespacio

RESUMEN EJECUTIVO

Hemos llegado al final de un período de veinticinco años de estabilidad estratégica y relativa paz entre las principales potencias. El conflicto entre Estados ha adoptado nuevas formas, y las actividades cibernéticas están jugando un papel destacado en este nuevo y volátil entorno. Durante la última década, el número y la sofisticación de los ciberataques por parte de actores estatales y no estatales han aumentado, amenazando así la estabilidad del ciberespacio. Dicho en pocas palabras, las personas y las organizaciones ya no pueden confiar en su capacidad para utilizar el ciberespacio de manera segura, ni en la disponibilidad e integridad de los servicios y la información.

En este contexto, se convocó la Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC) para que formulase recomendaciones para impulsar la ciberestabilidad. Empezamos identificando un marco de ciberestabilidad compuesto de siete elementos: 1) la participación de múltiples partes interesadas; 2) los principios de la ciberestabilidad; 3) la elaboración y aplicación de normas voluntarias; 4) la adhesión al derecho internacional; 5) las medidas encaminadas a generar confianza; 6) la creación de capacidades, y 7) la promulgación pública y el uso generalizado de normas técnicas que garanticen la resiliencia del ciberespacio. Tras definir este marco, la Comisión examinó a fondo tres de sus elementos: la participación de múltiples partes interesadas, los principios y las normas.

En muchos acuerdos internacionales se pide la participación de múltiples partes interesadas, pero este sigue siendo un asunto controvertido. Algunos continúan creyendo que garantizar la seguridad y la estabilidad internacionales es una responsabilidad casi exclusiva de los Estados. Sin embargo, en la práctica, los actores no estatales son principalmente los que diseñan, implantan y operan en el campo de batalla cibernético (es decir, el ciberespacio), y creemos que su participación es necesaria para garantizar la estabilidad del mismo. Por otra parte, su participación es inevitable, ya que los actores no estatales suelen ser los primeros en responder a los ciberataques, e incluso en atribuírselos.

La Comisión concluyó que dichos actores no estatales no solo eran fundamentales para garantizar la estabilidad del ciberespacio, sino que también debían guiarse por principios y estar obligados por normas. Los cuatro principios reflejan este punto de vista y hacen un llamamiento a todas las partes para que sean responsables, ejerzan moderación, tomen medidas y respeten los derechos humanos:

- Responsabilidad: Todos somos responsables de velar por la estabilidad del ciberespacio.
- Contención: Ningún Estado o actor no estatal debe tomar medidas que perjudiquen a la estabilidad del ciberespacio.
- Obligación de actuar: Los actores estatales o no estatales deben tomar medidas razonables y adecuadas para velar por la estabilidad del ciberespacio.
- Respeto a los Derechos Humanos: Los esfuerzos para garantizar la estabilidad del ciberespacio deben respetar los derechos humanos y el estado de derecho.

Sobre la base de estos principios, y tratando de complementar y no duplicar el trabajo de otros, la Comisión elaboró ocho normas diseñadas para mejorar la estabilidad del ciberespacio y abordar las preocupaciones técnicas o las lagunas en las normas promulgadas en ocasiones anteriores:

1. Los actores estatales y no estatales no deben llevar a cabo ni permitir a sabiendas actividades que dañen intencionadamente y de manera sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio.
2. Los actores estatales y no estatales no deben llevar a cabo, apoyar o permitir operaciones cibernéticas que tengan por objeto perturbar la infraestructura técnica esencial para la celebración de elecciones, referendos o plebiscitos.
3. Los actores estatales y no estatales no deben manipular los productos y servicios en el desarrollo y la producción, ni permitir que se manipulen, si al hacerlo pueden menoscabar sustancialmente la estabilidad del ciberespacio.

4. Los actores estatales y no estatales no deben apropiarse de los recursos de las TIC de uso público para utilizarlos como redes de bots o con fines similares.

5. Los Estados deben crear marcos transparentes en materia de procedimientos para evaluar si deben revelar las vulnerabilidades o fallos no conocidos por el público en los sistemas y tecnologías de la información de los que tengan conocimiento, y cuándo deben hacerlo. De manera predeterminada se debe abogar por la divulgación.

6. Los desarrolladores y fabricantes de productos y servicios de los que dependa la estabilidad del ciberespacio deben: 1) dar prioridad a la seguridad y la estabilidad, 2) tomar medidas razonables para garantizar que sus productos o servicios estén libres de vulnerabilidades importantes, y 3) tomar medidas para mitigar oportunamente las vulnerabilidades que se descubran posteriormente y ser transparentes en cuanto a su procedimiento. Todos los actores tienen el deber de compartir información sobre las vulnerabilidades para ayudar a prevenir o mitigar las actividades cibernéticas malintencionadas.

7. Los Estados deben promulgar medidas adecuadas, incluyendo leyes y reglamentos, para garantizar una higiene cibernética básica.

8. Los actores no estatales no deben participar en operaciones cibernéticas ofensivas y los actores estatales deben prevenir dichas actividades y actuar en caso de que se produzcan.

Recomendaciones

Por último, reconociendo tanto la importancia de la participación de múltiples partes interesadas como el hecho de que declarar un comportamiento como normativo no hace que lo sea, la Comisión formula seis recomendaciones centradas en fortalecer el modelo de múltiples partes interesadas, promover la adopción y aplicación de normas y garantizar que quienes las infrinjan rindan cuentas.

De manera específica, la Comisión recomienda que:

1. Los actores estatales y no estatales adopten y apliquen normas que mejoren la estabilidad del ciberespacio promoviendo la contención y fomentando la acción.

2. Los actores estatales y no estatales, en consonancia con sus responsabilidades y limitaciones, respondan adecuadamente a las infracciones de las normas, garantizando que aquellos que las infrinjan deban afrontar consecuencias previsibles y significativas.

3. Los actores estatales y no estatales, entre los que se incluyen las instituciones internacionales, redoblen sus esfuerzos por formar al personal, fomenten la capacidad y los medios, promuevan un conocimiento compartido de la importancia de la estabilidad del ciberespacio y tengan en cuenta las diversas necesidades de las distintas partes.

4. Los actores estatales y no estatales recopilen, compartan, estudien y publiquen información relacionada con infracciones de normas y el impacto resultante de dichas actividades.

5. Los actores estatales y no estatales establezcan y presten apoyo a las Comunidades de intereses para ayudar a garantizar la estabilidad del ciberespacio.

6. Se establezcan un mecanismo permanente de participación de múltiples partes interesadas para abordar cuestiones de estabilidad, en el que los Estados, el sector privado (incluida la comunidad técnica) y la sociedad civil participen y atiendan consultas de forma adecuada.

La publicación del presente informe supone tanto un fin como un comienzo. La Comisión ha cumplido su mandato. Sin embargo, para los miembros y colaboradores de la GCSC, así como para todos aquellos que apoyan sus objetivos, la ardua labor necesaria para implementar estos principios, normas y recomendaciones no ha hecho más que empezar. Y debe empezar, ya que los beneficios del ciberespacio se perderán si no se garantiza la estabilidad del mismo.

1. INTRODUCCIÓN

La evolución digital y el ciberespacio han transformado radicalmente la existencia del ser humano.[1] La capacidad de digitalizar, almacenar, analizar y transportar datos por todo el planeta ha tenido efectos profundos en todos los sectores de la sociedad y ha cambiado la forma en que nos ocupamos de los asuntos personales, empresariales y políticos. Hoy en día, cerca de la mitad de la población mundial tiene acceso a Internet[2] y este número aumenta rápidamente. Pero incluso aquellos que no están personalmente conectados al ciberespacio se ven afectados por su alcance, ya que las entidades de las que dependen para proporcionar bienes y servicios suelen utilizar el ciberespacio para las comunicaciones, la logística y las finanzas.

Los beneficios del ciberespacio, y la necesidad de garantizar su estabilidad, se han discutido a menudo, al igual que sus retos. Lo más destacable es que el ciberespacio puede servir para fines tanto nobles como innobles. Por ejemplo, la conectividad global, el anonimato y la falta de rastreabilidad permiten que las personas y las máquinas accedan a datos y sistemas sin necesidad de declarar su identidad, pero los delincuentes también pueden aprovechar esas características para cometer delitos con impunidad. Como resultado, los gobiernos, las empresas y las personas de todo el mundo deben enfrentarse a una serie de dilemas. A los gobiernos les interesa proteger el ciberespacio, prestar servicios públicos y promover otras actividades importantes (por ejemplo, la educación y la banca en línea), pero también les interesa promover los intereses de la seguridad nacional, incluidas las actividades de aplicación de la ley, los servicios de inteligencia y la capacidad militar. Las empresas, preocupadas por la protección de sus clientes, su reputación y sus beneficios, sufren ataques, deben investigar actividades malintencionadas y/o son objeto de solicitudes de datos por parte de instituciones públicas. Las personas, estén o no conectadas, dependen cada vez más de la tecnología digital y la adoptan, pero están preocupadas por su disponibilidad sin interrupciones y su integridad. Durante la última década, el número y la sofisticación de los ataques cibernéticos han aumentado, incluyendo los ataques a los sistemas de las administraciones públicas y a las infraestructuras críticas.[3] Así pues, no son alentadores ni el statu quo ni las tendencias que podemos observar.

Los ataques cibernéticos, llevados a cabo tanto por actores estatales como no estatales, ponen de manifiesto que el mundo necesita un marco de ciberestabilidad. Un tal marco servirá para reducir las posibilidades de que se produzcan alteraciones importantes del ciberespacio que mermen sus beneficios y reduzcan el bienestar de las personas, incluidos sus derechos y libertades. Sin duda, los productos y servicios bien diseñados y fabricados, y bien

1 El «Ciberespacio» se ha definido de varias maneras. https://es.wikipedia.org/wiki/Ciberespacio. Según la definición del diccionario, se trata de «an electronic system that allows computer users around the world to communicate with each other or to access informa-tion for any purpose» (un sistema electrónico que permite a los usuarios de ordenadores de todo el mundo comunicarse entre ellos o acceder a la información con cualquier propósito). https://dictionary.cambridge.org/us/dictionary/english/cyberspace. Según el Gobierno del Reino Unido, «Cyberspace is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services.» (Ciberespacio es el término utilizado para describir el soporte electrónico de las redes digitales utilizado para almacenar, modificar y comunicar la información. Incluye Internet, pero también otros sistemas de información que sirven de apoyo a las empresas, la infraestructura y los servicios). https://www.cpni.gov.uk/cyber. Como tal, cabe decir que es más amplio que Internet, el cual se describe popularmente como un «conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyan una red lógica única de alcance mundial». Véase https://es.wikipedia.org/wiki/Internet. Véase también el documento de debate de la Unión Internacional de Telecomunicaciones, «Defining the Internet» (mayo de 2013), https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx.

2 «Internet Usage Statistics», Internet World Stats, última modificación del 4 de octubre de 2019, https://internetworldstats.com/stats.htm.

3 Centro de Estudios Estratégicos e Internacionales (CSIS, por sus siglas en inglés), *Significant Cyber Incidents Since 2006*, https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf; Louis Marinos y Marco Lourenço, ed., *ENISA Threat Landscape Report 2018*, ENISA (Enero 2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; Abhishek Agrawal et al., *Microsoft Security Intelligence Report*, Vol. 24 (Diciembre 2018), https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original; Naciones Unidas, Asamblea General, *Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional: Informe del Secretario General*, A/74/120 (24 de junio de 2019), https://undocs.org/es/A/74/120.

gestionados por los profesionales de las tecnologías de la información y los usuarios de ordenadores, aumentarán la seguridad y la estabilidad, del mismo modo que los productos y servicios diseñados de forma deficiente o negligente, o las prácticas operativas deficientes o negligentes, las debilitarán. Pero no bastará con mejorar el desarrollo y las operaciones, especialmente si los actores estatales y no estatales perciben el ciberespacio como un campo de batalla en el que se puede lograr una ventaja política, militar o económica. Un atacante tenaz puede superar las medidas de seguridad, lo cual ha dado lugar al dicho «En Internet, el ataque supera a la defensa» y ha generado inestabilidad.[4] Así pues, es importante centrarse no solo en la tecnología sino también en el comportamiento: ¿cómo podemos fomentar que todos los actores se comporten de manera responsable para que mejoren la estabilidad del ciberespacio, en lugar de ponerla en peligro?

Para ayudar a responder a esta pregunta, varias entidades gubernamentales y no gubernamentales respaldaron la creación de la Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC, por sus siglas en inglés),[5] y señalaron que:

> Hemos llegado al final de un período de veinticinco años de estabilidad estratégica y relativa paz entre las principales potencias. Los conflictos entre Estados adoptarán nuevas formas, y es probable que las actividades cibernéticas desempeñen un papel destacado en este nuevo y volátil entorno, lo que aumentará el riesgo de menoscabar el uso pacífico del ciberespacio como medio para facilitar el crecimiento económico y la expansión de las libertades individuales.
>
> Para contrarrestar estos acontecimientos, la Comisión Mundial sobre la Estabilidad del Ciberespacio elaborará propuestas de normas y políticas para mejorar la seguridad y la estabilidad internacionales y servir de guía para un comportamiento responsable en el ciberespacio de los actores tanto estatales como no estatales. La GCSC hará participar a todas las partes interesadas en el desarrollo de un mutuo entendimiento, y su trabajo promoverá la ciberestabilidad mediante el apoyo al intercambio de información y la creación de capacidades, la investigación básica y la promoción.[6]

Es de destacar que la propia Comisión está formada por múltiples partes interesadas y es de ámbito global, ya que está integrada por personas con diversos antecedentes y conocimientos especializados. Algunos Comisionados han trabajado en administraciones públicas y han participado en negociaciones bilaterales y multilaterales sobre cuestiones cibernéticas, mientras que otros tienen experiencia en el desarrollo, el mantenimiento y la protección de la propia Internet. Otros han representado a la sociedad civil.

El trabajo de la Comisión no se desarrolla en el vacío y la GCSC, reconociendo que muchas otras instituciones y procesos (tanto pasados como presentes) comparten su interés por la estabilidad del ciberespacio, ha tratado de no duplicar el trabajo de otros. Más bien, la GCSC intenta basarse en otros procesos de múltiples partes interesadas y gubernamentales e influir en los trabajos futuros. Estos procesos incluyen la labor fundacional y en curso del Grupo de Expertos Gubernamentales de las

4 Véase, por ejemplo, P.W. Singer y Allan Friedman, «The Cult of the Cyber Offensive», *Foreign Policy* (15 de enero de 2014), https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/; Foro Económico Mundial (FEM), *The Global Risks Report 2019*, (2019), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

5 Para obtener más información sobre la GCSC, véase el Apéndice C: Historia, objetivos y procesos de la GCSC.

6 Comisión Mundial sobre la Estabilidad del Ciberespacio, https://cyberstability.org/.

7 La Asamblea General de las Naciones Unidas, en una importante resolución, ratificó unánimemente en 2015 la conclusión del Grupo de Expertos Gubernamentales de las Naciones Unidas. Véase la resolución 70/237 de la Asamblea General, *Resolución aprobada por la Asamblea General el 23 de diciembre de 2015 [sobre la base del informe de la Primera Comisión (A/70/455)]* , https://undocs.org/es/A/%20RES/70/237. Así pues, el derecho internacional y, en particular, el Estatuto de las Naciones Unidas establecen un marco exclusivo para la respuesta internacional a los actos hostiles, que se aplica también a las operaciones cibernéticas. Nuestro trabajo está basado en el acuerdo de todos los Estados de la Asamblea General de las Naciones Unidas de 2015 para guiarse por normas de comportamiento responsable con el fin de aumentar la estabilidad y la seguridad en el uso de las TIC y cumplir con sus compromisos bajo la ley internacional de diligencia debida y cooperación.

Naciones Unidas (UN GGE, por sus siglas en inglés),[7] la labor del Grupo de Trabajo de Composición Abierta (UN OEWG, por sus siglas en inglés), así como los esfuerzos del Foro Global de Especialistas en Ciberseguridad (GFCE, por sus siglas en inglés),[8] la Cumbre Mundial sobre la Sociedad de la Información (CMSI), la Comisión Mundial sobre la Gobernanza de Internet (Comisión Bildt), el Foro para la Gobernanza de Internet (FGI), la Conferencia Mundial sobre el Ciberespacio (CMC/Proceso de Londres), la Iniciativa NETmundial, la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Comisión de la Unión Africana (CUA), el Charter of Trust, el Cybersecurity Tech Accord, el Programa de La Haya sobre Normas Cibernéticas, el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR, por sus siglas en inglés), el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio («Llamamiento de París») y el Panel de Alto Nivel sobre Cooperación Digital del Secretario General de las Naciones Unidas. El trabajo de la Comisión también se basó en investigaciones encargadas y en solicitudes de comentarios públicos.

Algunos de los esfuerzos mencionados se centraban, en parte, en la estabilidad del ciberespacio, y preocupaba que la estabilidad y la gobernanza del ciberespacio estuvieran inextricablemente vinculadas. Es decir, en ausencia de un modelo de gobernanza robusto, la sociedad no dispone de las interacciones y los procesos de toma de decisiones necesarios para garantizar la estabilidad. Así, por ejemplo, la Comisión Bildt propuso un pacto social con múltiples partes interesadas para la privacidad y la seguridad digitales «entre los ciudadanos y sus representantes electos, la judicatura, los organismos policiales y los servicios de inteligencia, las empresas, la sociedad civil y la comunidad técnica de Internet, con el objetivo de restablecer la fiabilidad y aumentar la confianza en Internet».[9]

Encomiamos estos esfuerzos previos para desarrollar principios, reglas y normas a aplicar al comportamiento en el nuevo y turbulento dominio del ciberespacio, y creemos que es necesario un marco integral para aumentar la estabilidad del ciberespacio. Los antecedentes históricos demuestran que las sociedades y los gobiernos pueden, en algunos casos, tardar decenios en desarrollar estructuras internacionales de gobierno amplias y formales para las nuevas tecnologías disruptivas importantes.[10] El surgimiento del ciberespacio como una dimensión crucial en la interdependencia económica, social y de seguridad a nivel global apenas data de finales de los años 90, cuando comenzó el uso generalizado de la World Wide Web. Así pues, los procesos de gobernanza en desarrollo se encuentran en una fase temprana en la que coexisten áreas de coherencia e incoherencia normativas.[11] Por ejemplo, aunque las normas e instituciones relacionadas con el Sistema de Nombres de Dominio están bien desarrolladas, existen importantes áreas de desacuerdo entre los Estados y entre las empresas relacionadas con la regulación de contenidos. En ocasiones, los actores estatales y no estatales aplican normas de otros regímenes como el de la propiedad intelectual y el comercio y, cada vez más, son las propias empresas privadas las que fijan las normas.[12] El propósito de nuestra Comisión no es el de solucionar estas diversas cuestiones de gobernanza, sino el de situarlas en un marco general para asegurar la estabilidad del ciberespacio.

También constatamos que quienes se preocupan por la estabilidad del ciberespacio se han esforzado por estar a la altura de quienes tratan de debilitarlo, así como por seguir el ritmo de los avances tecnológicos y de la evolución de los conflictos geopolíticos. En parte, el desafío consiste en que el ciberespacio ha transformado la forma en que los actores persiguen objetivos políticos y militares; al ser las barreras de entrada bajas, es menos difícil convertirse en una ciberpotencia que en una potencia militar tradicional. Asimismo, al contar con estas nuevas tecnologías en su juego de herramientas, algunos vacilan en adoptar restricciones, en particular si esas restricciones no se respetan de forma generalizada. Se necesita un marco general de ciberestabilidad para la comunidad internacional que promueva la estabilidad del ciberespacio y que, al mismo tiempo, mantenga su utilidad a medida que siga aumentando el ritmo de los cambios tecnológicos. Por consiguiente, empezamos por definir el objetivo principal: proteger la estabilidad del ciberespacio.

8 El GFCE ha sido especialmente activo en el desarrollo de capacidades. Véase, por ejemplo, «Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building», Foro Global de Especialistas en Ciberseguridad (24 de noviembre de 2017), https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

9 Comisión Mundial sobre la Gobernanza de Internet, *One Internet* (2016), p. IX, https://www.cigionline.org/sites/default/files/gcig_ final_report_-_with_cover.pdf. «We call on governments, private corporations, civil society, the technical community and individ-uals together to create a new social compact for the digital age» (Hacemos un llamamiento a los gobiernos, las empresas privadas, la sociedad civil, la comunidad técnica y los individuos para que todos juntos creen un nuevo pacto social para la era digital).

10 Quizás el ejemplo más adecuado de una estructura de gobierno de este tipo es el relativo a las armas nucleares, cuya creación requirió un tiempo y un esfuerzo considerables. Incluso ahora, 60 años después del Tratado sobre la no proliferación de las armas nucleares (TNP), la gobernanza en materia de armas nucleares sigue siendo una preocupación en el ámbito de la seguridad.

11 Esta etapa temprana se ha denominado «regime complex» (complejo de regímenes). Véase Jo-seph Nye, «The Regime Complex for Managing Complex Global Cyber Activities», Comisión Mundial sobre la Gobernanza de Internet, N.º 1 (mayo de 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

12 Véase, por ejemplo, las normas desarrolladas por ISOC y Microsoft: «Mutually Agreed Norms for Routing Security (MANRS),» Internet Society (2014), https://www.manrs.org/; Angela McKay et al., *International Cybersecurity Norms Reducing Conflict in an Internet-dependent World*, Microsoft (Diciembre de 2014), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA; y Scott Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, Microsoft (Junio de 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

2. ¿QUÉ SE ENTIENDE POR ESTABILIDAD DEL CIBERESPACIO?

DEFINICIÓN:

La estabilidad del ciberespacio significa que todo el mundo puede confiar razonablemente en su capacidad para usar el ciberespacio de forma segura, estando la disponibilidad y la integridad de los servicios y la información proporcionados en el mismo y a través del mismo generalmente garantizadas, y en el que el cambio se gestiona de manera relativamente pacífica y las tensiones se resuelven sin recurrir a la escalada de tensiones.

Si bien la definición de la Comisión se basa en la definición estándar de «estabilidad»[13], presenta más matices en dos sentidos. En primer lugar, está la referencia a la confianza del usuario. La confianza es importante porque las decisiones de los seres humanos pueden basarse en percepciones y no solamente en hechos, y si alguien percibe una falta de estabilidad, puede ser reacio a utilizar el ciberespacio y beneficiarse del mismo. A modo de ejemplo, la utilización del ciberespacio puede optimizar los procesos y hacerlos más eficientes, lo que hace pensar que ciertas funciones (por ejemplo, el acceso a los servicios gubernamentales o la banca en línea) podrían verse beneficiadas al potenciar el mismo. Sin embargo, si esos sistemas no son fiables, o existe la percepción de que no son fiables, su uso será limitado y se perderán los beneficios de esta tecnología.

En segundo lugar, debe recordarse que el ciberespacio es un dominio sometido a cambios constantes. Se producen cambios en la tecnología, los modelos de negocio, la funcionalidad y las expectativas de la sociedad sobre el papel de la tecnología en la vida cotidiana. Por consiguiente, a diferencia de la definición de «estabilidad» del diccionario, que incluye el «retorno a una condición original», lo que necesitamos son mecanismos ágiles para asegurar la estabilidad del ciberespacio a medida que las tecnologías evolucionan. Dicho de manera sencilla, es preciso que todos sigan confiando en la disponibilidad e integridad del ciberespacio, incluso cuando este y el mundo que lo rodea cambien.

13 «Estabilidad» se define como la «cualidad de estable». https://lexico.com/es/definicion/estabilidad. Estable significa: 1) no susceptible de ceder o volcar; firmemente fijado; 2) no susceptible de cambiar o fallar; firmemente establecido; y 3) no sujeto a cambios físicos. Véase https://en.oxforddictionaries.com/definition/stable. En las relaciones internacionales, una de las definiciones más coherentes del término estabilidad internacional es «the probability that the [international] system retains all of its essential characteristics; that no single nation becomes dominant; that most of its members continue to survive; and that large-scale war does not occur» (la probabilidad de que el sistema [internacional] conserve todas sus características esenciales, de que ninguna nación individual llegue a ser dominante, de que la mayoría de sus miembros sigan sobreviviendo, y de que no se produzca una guerra a gran escala). Karl W. Deutsch y J. David Singer, «Multipolar Power Systems and International Stability,» *World Politics*, Vol. 16, No. 3 (Abril de 1964): 390-406, http://users.metu.edu.tr/utuba/Deutsch.pdf.

3. EL MARCO DE LA CIBERESTABILIDAD DE LA GCSC

Para hacer frente a los desafíos anteriormente descritos, la GCSC, al igual que otros[14], propone un marco integral de ciberestabilidad. Este marco incluye: 1) la participación de múltiples partes interesadas; 2) los principios de la ciberestabilidad; 3) la elaboración y aplicación de normas voluntarias; 4) la adhesión al derecho internacional; 5) las medidas encaminadas a generar confianza; 6) la creación de capacidades, y 7) la promulgación pública y el uso generalizado de normas técnicas que garanticen la resiliencia del ciberespacio. Los esfuerzos de la GCSC se han centrado principalmente en tres de estos temas (el enfoque con múltiples partes interesadas, los principios y las normas) y estos se tratan en las secciones 4, 5 y 6, respectivamente. En lo que respecta a las normas, nos centramos no solo en su elaboración, sino también en cuestiones más difíciles como la adopción, la aplicación y la rendición de cuentas de los infractores.

Cabe señalar que actualmente se están realizando muchos esfuerzos para tratar los elementos individuales de este marco para la ciberestabilidad y que esos esfuerzos son, como el propio ciberespacio, descentralizados. La GCSC considera que para avanzar se requiere un esfuerzo concertado de múltiples partes interesadas a nivel mundial. Por lo tanto, la GCSC no solamente se ocupa de las cuestiones sustantivas, sino que también hace recomendaciones sobre procesos, con las que intenta aprovechar y complementar los esfuerzos existentes y, tal vez, darles un nuevo impulso.

14 Véase, por ejemplo, *The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation* (Junio de 2019), pág. 39, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf. «We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action» (Recomendamos el desarrollo de un Compromiso Mundial sobre Confianza y Seguridad Digital para dar forma a una visión compartida, identificar los atributos de la estabilidad digital, elucidar y fortalecer la aplicación de normas para el uso responsable de la tecnología y proponer prioridades de acción).

4. COMPROMISO DE LAS MÚLTIPLES PARTES INTERESADAS

A pesar de la gran cantidad de acuerdos internacionales entre los Estados en los que se cita la importancia de un enfoque de múltiples partes interesadas, este sigue siendo un tema polémico. Para algunos, el debate es filosófico y se centra en el contraste de papeles que los actores estatales y no estatales desempeñan en la política tecnológica y los asuntos internacionales. Para otros, los procesos con múltiples partes interesadas son prácticos, y sostienen que los Estados que actúan solos o con un mínimo de aportaciones no estatales no pueden asegurar la estabilidad del ciberespacio.[15] Estamos de acuerdo con este último punto de vista.

El tema de los méritos de la participación de múltiples partes interesadas se lleva debatiendo decenios. A menudo, el asunto se planteaba en el contexto de la gestión de los recursos de Internet, pero también se planteaba la cuestión de las normas y la seguridad nacional. Por ejemplo, durante la segunda fase de la Cumbre Mundial sobre la Sociedad de la Información de las Naciones Unidas, el Grupo de Trabajo de las Naciones Unidas sobre la Gobernanza de Internet (GTGI) rechazó el concepto de liderazgo de una sola parte interesada. Por el contrario, llegó a la conclusión de que Internet es demasiado grande para ser administrada por un solo grupo de partes interesadas o una sola organización, y propuso un enfoque de múltiples partes interesadas. Así pues, en 2005, los Jefes de Estado participantes en la Agenda de Túnez de la Cumbre Mundial sobre la Sociedad de la Información declararon que «una definición de trabajo del concepto de gobernanza de Internet es el desarrollo y la aplicación por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivas funciones, de principios, normas, reglas, procedimientos para la toma de decisiones y programas compartidos que configuran la evolución y el uso de Internet».[16]

Diez años más tarde, la Reunión de Alto Nivel de la Asamblea General de las Naciones Unidas sobre la revisión general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información reafirmó este punto de vista y también declaró lo siguiente en la resolución 70/125 (2015) de las Naciones Unidas:

> Reafirmamos, además, el valor y los principios de la cooperación y la participación de múltiples partes interesadas que han caracterizado el proceso de la Cumbre Mundial de la Sociedad de la Información desde sus inicios, reconociendo que la participación, la asociación y la cooperación efectivas de los gobiernos, el sector privado, la sociedad civil, las organizaciones internacionales, las comunidades técnica y académica y todas las demás partes interesadas pertinentes, en el marco de sus funciones y responsabilidades respectivas, en particular con una representación equilibrada de los países en desarrollo, ha sido y sigue siendo vital para el desarrollo de la sociedad de la información.[17]

15 «The WSIS definition (2005) introduced the concept of the 'respectiveroles' and the philosophy of 'sharing'. The NETmundial Declaration (2014) defined key elements as bottom up, openness, transparency, inclusiveness and human rights based. In other words, we have some general guidelines for a multistakeholder approach, but we do not have a single multistakeholder model. So far, two different multistakeholder models have emerged: the consultative model and the collaborative model.» (La definición de la Cumbre Mundial sobre la Sociedad de la Información (2005) introdujo el concepto de los 'papeles respectivos' y la filosofía de 'compartir'. La Declaración de NETmundial (2014) definió como elementos clave la participación de abajo hacia arriba, la apertura, la transparencia, la inclusión y los derechos humanos. En otras palabras, tenemos algunas directrices generales para un enfoque con múltiples partes interesadas, pero no tenemos un modelo único de múltiples partes interesadas. Hasta la fecha, han surgido dos modelos diferentes de múltiples partes interesadas: el modelo consultivo y el modelo de colaboración.) Wolfgang Kleinwächter, «Towards a Holistic Approach for Internet Related Public Policy Making,» Comisión Mundial sobre la Estabilidad del Ciberespacio (Enero de 2018), https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf. Para una discusión adicional sobre los modelos de múltiples partes interesadas, véase Virgilio Almeida et al., «The Origin and Evolution of Multistakeholder Models», *IEEE Internet Computing*, Vol. 19 (Enero-Febrero de 2015): 74-79, https://doi.ieee-computersociety.org/10.1109/MIC.2015.15.

16 «Tunis Agenda for the Information Society», Cumbre Mundial sobre la Sociedad de la Información (18 de noviembre de 2005), Párrafo 34, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

17 Véase la resolución 70/125 de la Asamblea General de las Naciones Unidas, *Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información*, A/RES/70/125 (16 de diciembre de 2015), Párrafo 3, https://undocs.org/es/A/RES/70/125.

Una vez más, la declaración fue más allá de la gestión de los recursos críticos de Internet y pasó directamente al meollo de las cuestiones de seguridad nacional:

> Reconocemos la función de liderazgo de los gobiernos en las cuestiones de ciberseguridad relativas a la seguridad nacional. Reconocemos también las importantes funciones y contribuciones de todas las partes interesadas, de conformidad con sus respectivas funciones y responsabilidades.[18]

En cuanto a las normas en particular, el Grupo de los Ocho (G8) declaró en 2011 que:

> La seguridad de las redes y los servicios en Internet es una cuestión que concierne a múltiples partes interesadas. Requiere una coordinación entre los gobiernos, las organizaciones regionales e internacionales, el sector privado, [y] la sociedad civil... Los gobiernos tienen una función que desempeñar, sobre la base de la información aportada por un amplio abanico de partes interesadas, para ayudar a elaborar normas de comportamiento y enfoques comunes en la utilización del ciberespacio.[19]

Dos años después, en 2013, el Grupo de Expertos Gubernamentales de las Naciones Unidas emitió su *Informe sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* . En una sección titulada «Fomento de la cooperación para lograr un entorno pacífico, seguro, resistente y abierto para las tecnologías de la información y las comunicaciones», el Grupo de Expertos Gubernamentales de las Naciones Unidas señaló que «[s]i bien los Estados deben liderar la labor destinada a afrontar estos desafíos, una participación apropiada del sector privado y la sociedad civil mejoraría la cooperación».[20] El informe continuó diciendo, en una sección titulada «Recomendaciones sobre normas, reglas y principios de conducta estatal responsable», que:

> Los Estados Miembros deberían examinar cuál es la mejor forma de cooperar para aplicar las normas y principios de conducta responsable antes señalados, incluida la función que podrían asumir el sector privado y las organizaciones de la sociedad civil.[21]

Estas posiciones fueron reafirmadas en el informe de 2015 del Grupo de Expertos Gubernamentales de las Naciones Unidas, donde se declaró que:

> Si bien los Estados tienen la responsabilidad primordial de garantizar un entorno seguro y pacífico en la esfera de las TIC, la eficacia de la cooperación internacional mejoraría si se establecieran mecanismos para la participación, según procediera, del sector privado, el mundo académico y las organizaciones de la sociedad civil.[22]

Esta declaración se repitió en una resolución de la Asamblea General de 2018 sobre *Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional*.[23] Otros acuerdos internacionales expresan claramente el mismo sentimiento; por ejemplo, el Llamamiento de París declaró: «Reconocemos la necesidad de fortalecer el enfoque de múltiples partes interesadas y de realizar esfuerzos adicionales para disminuir los riesgos para la estabilidad del ciberespacio y para fomentar la confianza, la capacidad y la fiabilidad».[24]

18 Id., párrafo 50.
19 Grupo de los Ocho, «G8 Declaration: Renewed Commitment for Freedom and Democracy», Cumbre del G8 en Deauville (27 de mayo de 2011), Párrafo 17, http://www.g8.utoronto.ca/summit/2011deau-ville/2011-declaration-en.html.
20 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/68/98 (24 de junio de 2013), pág. 7, párrafo 12, https://undocs.org/es/A/68/98, (en adelante, Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2013).
21 Id., pág. 8, párrafo 25.
22 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/70/174 (22 de julio de 2015), pág. 13, párr. 31, https://undocs.org/es/A/70/174, (en adelante, Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015).
23 Resolución 73/266 de la Asamblea General de las Naciones Unidas, *Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional*, A/RES/73/266 (22 de diciembre de 2018), https://undocs.org/es/A/RES/73/266.
24 «Ministerio para la Confianza y Seguridad en el Ciberespacio» (11 de noviembre de 2018), https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918. pdf. Véase también, NETmundial, «NETmundial Multistakeholder Statement» (24 de abril de 2014), http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Más recientemente, en junio de 2019, el Panel de Alto Nivel sobre Cooperación Digital del Secretario General de las Naciones Unidas, en su informe *The Age of Digital Interdependence*, declaró:

> La cooperación digital eficaz requiere que se fortalezca el multilateralismo, a pesar de las tensiones actuales. También es preciso que el multilateralismo se complemente con la cooperación entre múltiples partes interesadas, en la que participen no solo los gobiernos sino un espectro mucho más diverso de partes interesadas de otra índole, como la sociedad civil, los académicos, los técnicos y el sector privado.[25]

Si bien la idea de un enfoque basado en la participación de múltiples partes interesadas ha demostrado tener éxito, no cuenta con un apoyo universal. Algunos gobiernos siguen creyendo que garantizar la seguridad y la estabilidad internacionales es responsabilidad casi exclusiva de los Estados. Esta visión más tradicional de la seguridad nace de la noción de que los Estados tienen la responsabilidad de proteger a sus ciudadanos de los ataques por la fuerza, idea plasmada en las responsabilidades del Consejo de Seguridad de las Naciones Unidas según lo dispuesto en el Artículo 24 de la Carta de las Naciones Unidas.[26] También es posible que esta línea de pensamiento se vea reforzada por las experiencias del pasado porque, en el ámbito físico, los gobiernos no solo disfrutaban del monopolio del uso legítimo de la fuerza, sino que también controlaban las armas de uso militar (por ejemplo, aviones, tanques) que se utilizaban para atacar y defender ese dominio.

En la práctica, es el sector privado el que diseña, despliega y opera en el campo de batalla cibernético (es decir, el ciberespacio). Los gobiernos no son, a pesar de sus responsabilidades únicas, los protectores exclusivos de este dominio. Incluso si los gobiernos mantienen un monopolio *de jure* sobre el uso legítimo de la fuerza en el ciberespacio, ya no tienen un monopolio práctico sobre el ataque y la protección de este dominio, ni pueden impedir la proliferación y el uso de poderosas armas cibernéticas. Por el contrario, la comunidad técnica, la sociedad civil y los individuos también desempeñan un papel importante en la protección del ciberespacio, incluida la promulgación de normas. Por lo tanto, el enfoque de múltiples partes interesadas es necesario para mejorar los resultados y asegurarse de que las normas y políticas que respaldan la estabilidad del ciberespacio estén bien formuladas y eviten consecuencias indeseadas.

Igualmente importante es que, aunque los Estados deseen ir solos, no pueden. La participación de actores no estatales en asuntos que afectan a la estabilidad del ciberespacio es inevitable. Por ejemplo, muchos miembros del sector privado y de la comunidad técnica pueden ser responsables de protocolos y servicios críticos y pueden proteger a los Estados que utilizan sus productos comerciales y de código abierto. Además, incluso la investigación y la atribución de los ataques, tradicionalmente una función y una prerrogativa política de los gobiernos, ha dejado de ser su área de conocimiento y responsabilidad exclusiva; algunos ataques estatales importantes han sido identificados y divulgados por entidades no gubernamentales. En resumen, aunque los Estados tienen una función única que desempeñar durante y después de un ataque (incluidas las actividades de aplicación de la ley y/o la adopción de medidas diplomáticas o de otro tipo por parte del Estado), no tienen el monopolio de la investigación y la atribución, ni pueden excluir en la práctica a los actores no estatales. En consecuencia, la elaboración de normas y políticas exitosas sobre el ciberespacio, y la garantía de su cumplimiento, requiere la participación de todas las partes interesadas, en los cuales recae la responsabilidad, y los gobiernos deben centrarse en la creación de mecanismos que incluyan efectivamente la participación del sector privado, la comunidad técnica, las instituciones académicas y otros representantes de la sociedad civil. Esto es exactamente lo que muchos gobiernos han solicitado.

25 *The Age of Digital Interdependence*, pág. 7, https://digitalcooper-ation.org/wp-content/uploads/2019/06/DigitalCooperation-re-port-web-FINAL-1.pdf.

26 Carta de las Naciones Unidas, «Capítulo V: El Consejo de Seguridad», Repertorio de la práctica seguida por los órganos de las Naciones Unidas, http://legal. un.org/repertory/art24.shtml.

5. PRINCIPIOS

El comportamiento normativo deriva de los valores. Por lo tanto, nuestro punto de partida debe ser la declaración de esos valores, ya sea los referentes a las responsabilidades individuales, a las responsabilidades del Estado o a los derechos humanos fundamentales. En efecto, los diferentes valores pueden dificultar el logro de un consenso, así como dar lugar a diferentes interpretaciones y aplicaciones nacionales o regionales de los acuerdos internacionales. Esto no significa que se requiera un acuerdo sobre los principios para que se pueda avanzar; a veces, las partes se ponen de acuerdo sobre conductas aceptables aunque sus motivos para hacerlo difieran. Sin embargo, los principios compartidos y la interdependencia pueden conducir a compromisos más profundos y reducir el riesgo de futuros desacuerdos o conflictos. Por lo tanto, es importante que las partes celebren debates sinceros sobre los principios de alto nivel que guían su pensamiento y de los que emanan las normas.

Los siguientes cuatro principios son fundamentales para asegurar la estabilidad del ciberespacio:

1. **Responsabilidad:** Todos somos responsables de velar por la estabilidad del ciberespacio.
2. **Contención:** Ningún Estado o actor no estatal debe tomar medidas que perjudiquen a la estabilidad del ciberespacio.
3. **Obligación de actuar:** Los actores estatales o no estatales deben tomar medidas razonables y adecuadas para velar por la estabilidad del ciberespacio.
4. **Respeto a los Derechos Humanos:** Los esfuerzos para garantizar la estabilidad del ciberespacio deben respetar los derechos humanos y el estado de derecho.

A. El principio de responsabilidad

El primer principio trata de la naturaleza descentralizada y distribuida del ciberespacio. Reafirma la necesidad de un enfoque de múltiples partes interesadas para asegurar la estabilidad del ciberespacio y, especialmente, amplía el concepto de «partes interesadas» para incluir a todos los individuos. Cada individuo tiene la responsabilidad, a título personal y/o profesional, de asegurar la estabilidad del ciberespacio. Aunque pueda resultar obvio que los responsables de las políticas cibernéticas de los gobiernos y los empleados que gestionan los servicios en la nube desempeñan un papel, cada individuo conectado al ciberespacio debe hacer esfuerzos razonables para asegurar que sus propios dispositivos no se vean comprometidos y puedan ser utilizados en ataques. Incluso los que no están conectados a Internet quizá dependan de la red para recibir bienes y servicios, y a ellos también les interesa que la política sobre el ciberespacio se aborde adecuadamente en sus comunidades.

B. El principio de contención

El segundo principio contiene un requisito general de contención. Para los Estados, esto es consistente con las resoluciones de 2018 de la Asamblea General de las Naciones Unidas (AGNA) concernientes al comportamiento responsable del Estado en el ciberespacio[27] y el informe de 2015 del Grupo de Expertos Gubernamentales de las Naciones Unidas en el que se señala que «Los Estados, en consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, deberían... 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»[28] Pero no se trata solo de los Estados, ya que los actores no estatales también pueden llevar a cabo acciones, como hackear a sus atacantes, que también podrían debilitar la estabilidad del ciberespacio.

27 Resolución 73/27 de la Asamblea General de las Naciones Unidas, *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/RES/73/27 (5 de diciembre de 2018), https://undocs.org/es/A/RES/73/27; y la resolución 73/266 de la Asamblea General de las Naciones Unidas, https://undocs.org/es/A/RES/73/266.

28 Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015, pág. 7, párrafo 13 (a), https://undocs.org/es/A/70/174.

C. El principio de la obligación de actuar

El tercer principio contiene el requisito general de adoptar medidas positivas para preservar la estabilidad del ciberespacio. Al actuar, los Estados deben procurar evitar que las tensiones aumenten involuntariamente o que se incremente la inestabilidad. Esto es coherente con la obligación señalada en el informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015 de «cooperar en la elaboración y aplicación de medidas para aumentar la estabilidad y la seguridad en la utilización de las TIC.»[29] Pero, una vez más, no se trata solamente de los Estados, ya que las empresas privadas y los individuos también pueden tomar medidas de cooperación para ayudar a asegurar la estabilidad del ciberespacio. Por ejemplo, las empresas privadas pueden colaborar para mitigar las amenazas cibernéticas, y los particulares pueden asegurarse de que están empleando las mejores prácticas, como actualizaciones, parches y el uso de la autenticación multifactorial, para reducir el riesgo de que las redes de bots se apoderen de sus máquinas y se utilicen para lanzar ataques de gran alcance que amenacen la estabilidad del ciberespacio.

D. El principio de los derechos humanos

El cuarto principio reconoce la importancia de salvaguardar los derechos humanos como un elemento importante de la estabilidad del ciberespacio. A medida que aumenta la dependencia de las personas respecto de las tecnologías de la información y las comunicaciones, se amplifica el efecto perturbador en la actividad humana resultante de las amenazas a su disponibilidad o integridad. Por consiguiente, es imprescindible que, cuando los Estados persigan sus intereses estratégicos nacionales en el ciberespacio, presten la debida atención a las repercusiones resultantes en los individuos, en particular sus derechos humanos. Del mismo modo, los actores no estatales deberían considerar y reducir al mínimo los riesgos que sus actividades suponen para el disfrute de los derechos de las personas en línea y fuera de línea. Como mínimo, el cumplimiento del principio de los Derechos Humanos requiere que los Estados cumplan sus obligaciones en materia de derechos humanos en virtud del derecho internacional al realizar actividades en el ciberespacio.

Los derechos humanos universalmente aceptados han sido consagrados en la Declaración Universal de Derechos Humanos.[30] Además, se ha adoptado un gran número de acuerdos internacionales que prevén diversos derechos humanos específicos y crean obligaciones jurídicas vinculantes para los Estados participantes. En el contexto del ciberespacio, la Asamblea General de las Naciones Unidas ha confirmado explícitamente en varias ocasiones la aplicabilidad de las normas internacionales de derechos humanos,[31] el Consejo de Derechos Humanos de la ONU (HRC por sus siglas en inglés),[32] así como los informes del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2013 y 2015.[33] La defensa de los derechos y la confianza de los usuarios en el respeto de sus derechos es fundamental para garantizar la estabilidad del ciberespacio.

Cabe señalar que los cuatro principios no pretenden ser exhaustivos ni abarcar todos los aspectos de la política sobre el ciberespacio, y hay muchas organizaciones que han elaborado conjuntos de principios amplios que abarcan una gran variedad de cuestiones. También hay otras organizaciones dedicadas a cuestiones relacionadas con la gobernanza de Internet y los derechos humanos en línea (incluidas la privacidad, la libertad de expresión y la libertad de asociación). Nuestro objetivo es lograr una amplia aceptación de los principios que favorecen la estabilidad del ciberespacio, especialmente en una era sin precedentes de actividad hostil sofisticada en la que las normas pueden no estar claras o, aunque lo estén, puede que no sean aceptadas ni aplicadas.

29 Id.

30 Resolución 217 A (III) de la Asamblea General de las Naciones Unidas, *Declaración Universal de Derechos Humanos* (10 de diciembre de 1948), https://www.un.org/es/universal-declaration-human-rights//.

31 Véase la resolución 68/167 de la Asamblea General de las Naciones Unidas, *El derecho a la privacidad en la era digital*, A/RES/68/167 (18 de diciembre de 2013), https://undocs.org/es/A/RES/68/167; y la resolución 69/166 de la Asamblea General de las Naciones Unidas, *El derecho a la privacidad en la era digital*, A/RES/69/166 (18 de diciembre de 2014), https://undocs.org/es/A/RES/69/166.

32 Consejo de Derechos Humanos de las Naciones Unidas, *Promoción, protección y disfrute de los derechos humanos en Internet*, A/HRC/20/L.13 (29 de junio de 2012), https://undocs.org/es/A/HRC/20/L.13.

33 Informe del Grupo de Expertos Gubernamentales de la ONU de 2013, https://undocs.org/es/A/68/98 y el informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015, https://undocs.org/es/A/70/174.

6. NORMAS

Si bien los principios son un punto de partida clave para la elaboración de políticas y la orientación de las acciones tácticas, su alto nivel de abstracción requiere que se complementen con acuerdos más granulares que definan cuál es el comportamiento aceptable. Esto significa que los principios deben complementarse con normas. Las normas representan comportamientos sociales previstos y adecuados.[34] Es imposible hablar de las normas sin hacer referencia al trabajo de otras organizaciones, especialmente el Grupo de Expertos Gubernamentales de las Naciones Unidas y su informe de 2015.[35] El Grupo de Expertos Gubernamentales de las Naciones Unidas reconoció que «Teniendo en cuenta los atributos singulares de las TIC, con el tiempo podrían elaborarse más normas»,[36] y el mandato de la GCSC era, de hecho, «desarrollar propuestas de normas y políticas para mejorar la seguridad y estabilidad internacionales». Para basarse en los trabajos anteriores e identificar los casos en los que se pueden justificar normas adicionales, es importante comenzar a partir de las normas acordadas en 2015, que pueden encontrarse, en su totalidad, en el Apéndice A.

Como señaló el Grupo de Expertos Gubernamentales de las Naciones Unidas en 2015, se le encomendó, entre otras cosas, «señalar los ámbitos en que es preciso elaborar normas complementarias que tengan en cuenta la complejidad y las características singulares de estas tecnologías».[37] Desde entonces, los productos y servicios de las TIC, así como su mal uso, han seguido cambiando. Para abordar esta cuestión, la GCSC se centró en cubrir las lagunas del actual conjunto de normas, añadir concreción técnica al debate sobre las normas y abordar las cuestiones de su aplicación. Con respecto a cubrir las lagunas, por ejemplo, la GCSC aprobó una norma para proteger el núcleo público de Internet[38] y una norma para proteger los sistemas electorales.[39] Del mismo modo, mientras que la norma del Grupo de Expertos Gubernamentales de las Naciones Unidas se refiere a la «integridad de la cadena de suministro»,[40] una norma de la GCSC se refiere más específicamente a los tipos de ataques a la cadena de suministro que deben abordarse.[41]

34 https://en.oxforddictionaries.com/definition/norm.
35 Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015, https://undocs.org/es/A/70/174.
36 Id., p.8, párrafo 15.
37 Id., p.7, párrafo 11.

38 Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC, por sus siglas en inglés), *Call to Protect the Public Core of the Internet* (Convocatoria de protección del núcleo público de Internet) (Nueva Delhi, noviembre de 2017), https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf. El investigador neerlandés Dennis Broeders ha sido uno de los primeros defensores de la identificación de la necesidad de protección especial del núcleo público de Internet. Véase Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (El núcleo público de Internet: agenda internacional para la gobernanza de Internet) (Ámsterdam: Amsterdam University Press, 2015), http://www.oapen.org/download?type=document&docid=610631.
39 Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC), *Call to Protect the Electoral Infrastructure* (Llamamiento a la protección de la infraestructura electoral) (Bratislava, mayo de 2018), https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.
40 Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015, p.8, párrafo 13(i). «Los Estados deben tomar medidas razonables para garantizar la integridad de la cadena de suministro para que el usuario final pueda confiar en la seguridad de los productos de TIC. Los Estados deben tratar de evitar la proliferación de herramientas y técnicas de TIC malintencionadas, así como el uso de funciones ocultas peligrosas».
41 Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC), *Norms Through Singapore* (Normas por Singapur) (noviembre de 2018), https://cyberstabil-ity.org/wp-content/uploads/2019/04/singaporenew-digital.pdf. «Los actores estatales y no estatales no deben manipular el desarrollo y producción de productos y servicios, ni permitir dicha manipulación, si de este modo puede mermarse de forma importante la estabilidad del ciberespacio.

La otra gran diferencia entre las normas del Grupo de Expertos Gubernamentales de las Naciones Unidas y las normas propuestas por la GCSC es que esta última considera que también deben imponerse responsabilidades a los actores no estatales, ya que estos deben actuar con moderación o tomar medidas afirmativas para garantizar la estabilidad del ciberespacio. No nos referimos aquí a los ciberataques de los criminales; los criminales a los que no disuade la acción del gobierno no serán disuadidos por las normas. Pero como la tecnología cambia rápidamente y las leyes no, es útil ser preciso sobre qué conductas no estatales deben ser alentadas o desalentadas incluso en ausencia de leyes. Por ejemplo, algunos abogan por que se permita que las víctimas de hacking «respondan con hacking». Incluso en ausencia de leyes que permitan o prohíban dicha conducta, la GCSC la considera desaconsejable por varios motivos, entre ellos el hecho de que el atacante inicial puede estar enrutando su ataque a través de sistemas de terceros (por ejemplo, un proveedor en la nube o un hospital) y, por lo tanto, el hacking en respuesta puede afectar a usuarios inocentes (por ejemplo, clientes de la nube o pacientes). Además, como consecuencia de estos ataques a víctimas inocentes, el hacking en respuesta puede ser considerado como una escalada, o provocarla. En resumen, debido a las complejidades planteadas, incluso en ausencia de leyes, una norma que limite a los actores del sector privado puede influir en los comportamientos y, por lo tanto, servir a un propósito saludable.

A. Las normas propuestas por la GCSC

Teniendo en cuenta los puntos anteriores, la GCSC elaboró y propuso las siguientes normas:

1. Los actores estatales y no estatales no deben llevar a cabo ni permitir a sabiendas actividades que dañen intencionadamente y de manera sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio.

2. Los actores estatales y no estatales no deben llevar a cabo, apoyar o permitir operaciones cibernéticas que tengan por objeto perturbar la infraestructura técnica esencial para la celebración de elecciones, referendos o plebiscitos.

3. Los actores estatales y no estatales no deben manipular los productos y servicios en desarrollo y en producción, ni permitir que se manipulen, si al hacerlo pueden menoscabar sustancialmente la estabilidad del ciberespacio.

4. Los actores estatales y no estatales no deben apropiarse de los recursos de las TIC de uso público para utilizarlos como redes de bots o con fines similares.

5. Los Estados deben crear marcos transparentes en materia de procedimientos para evaluar si deben revelar las vulnerabilidades o fallos no conocidos por el público en los sistemas y tecnologías de la información de los que tengan conocimiento, y cuándo deben hacerlo. De manera predeterminada se debe abogar por la divulgación.

6. Los desarrolladores y fabricantes de productos y servicios de los que dependa la estabilidad del ciberespacio deben: 1) dar prioridad a la seguridad y la estabilidad, 2) tomar medidas razonables para garantizar que sus productos o servicios estén libres de vulnerabilidades importantes, y 3) tomar medidas para mitigar oportunamente las vulnerabilidades que se descubran posteriormente

y ser transparentes en cuanto a su procedimiento. Todos los actores tienen el deber de compartir información sobre las vulnerabilidades para ayudar a prevenir o mitigar las actividades cibernéticas malintencionadas.

7. Los Estados deben promulgar medidas adecuadas, incluyendo leyes y reglamentos, para garantizar una higiene cibernética básica.

8. Los actores no estatales no deben participar en operaciones cibernéticas ofensivas y los actores estatales deben prevenir dichas actividades y actuar en caso de que se produzcan.

Merece la pena señalar que puede resultar difícil encontrar el lenguaje más adecuado para expresar una norma. Si las normas son demasiado precisas y no dejan margen para la interpretación, puede ser difícil lograr un consenso y puede haber importantes lagunas en la cobertura. Por otra parte, si las normas son demasiado vagas, no proporcionan el tipo de orientación necesaria para guiar el comportamiento y establecer expectativas claras para un grupo específico de actores. El objetivo es encontrar un equilibrio adecuado y elaborar nuevas normas, cuando sea necesario, para garantizar que se tratan los comportamientos no deseados. A modo de ejemplo, las normas del Grupo de Expertos Gubernamentales de las Naciones Unidas aprobadas en 2015 protegían las infraestructuras críticas, pero no está claro que ese término abarque el núcleo público de Internet; muchos consideran que las infraestructuras críticas son los servicios públicos y las prestaciones de servicios (por ejemplo, energía, comunicaciones y banca).[42] Además, el Grupo de Expertos Gubernamentales de las Naciones Unidas no hizo referencia específicamente a los sistemas electorales, una preocupación que se agudizó después de 2015.[43] Si bien los sistemas electorales pueden estar contemplados en algunos países por referencia (es decir, algunos Estados consideran ahora que los sistemas electorales son una infraestructura crítica, lo cual los sitúa en el ámbito de las normas relativas a la infraestructura crítica),[44] es posible que algunos países no sigan este enfoque. Así pues, si bien el ciberespacio es mundial, es posible que las protecciones normativas no lo sean. Para contribuir al tratamiento de las cuestiones de interpretación relativas a las normas de la GCSC, la Comisión decidió proporcionar un texto de referencia para cada una de las normas descritas anteriormente (véase el Apéndice B).

Por último, las normas de comportamiento en el ciberespacio no pueden ser estáticas. Las normas de la GCSC reflejan un momento en el tiempo en un panorama tecnológico en constante cambio. Los actores estatales y no estatales deben estar preparados para desarrollar nuevas normas a medida que avanzan las tecnologías, y a medida que cambia nuestra comprensión acerca de las implicaciones de las tecnologías existentes.

Ya sea que se centren en las normas del Grupo de Expertos Gubernamentales de las Naciones Unidas, en las normas de la GCSC, o en otras propuestas, debe reconocerse que para que estas sean efectivas, es necesario que se adopten e implementen, y que los infractores de las mismas tengan que rendir cuentas. Ahora nos ocuparemos de esas cuestiones, antes de pasar a la forma en que los actores no estatales, que están descentralizados y distribuidos por todo el mundo, pueden reunirse para trabajar con los gobiernos en soluciones prácticas a los problemas de la ciberestabilidad.

B. Adopción de las normas

Para que una norma sea efectiva, debe lograr una amplia aceptación. Dicha aceptación, incluso por parte de actores que algunos consideran potenciales infractores de las normas, refuerza la legitimidad de las medidas que denuncian las infracciones de las normas y de las medidas colectivas apropiadas adoptadas para responder a dichas infracciones. Si bien lo mejor es una adopción generalizada, cabe la posibilidad de que grupos más pequeños de Estados u otras entidades de ideas afines se pongan de acuerdo sobre normas concretas y las hagan cumplir. Para abordar esta cuestión, la GCSC

42 Se ha definido la infraestructura crítica como la que incluye «sistemas y activos, ya sean físicos o virtuales, de importancia tal que la incapacidad o destrucción de los mismos podría ejercer un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o la seguridad pública nacional, o cualquier combinación de dichos aspectos». *Critical Infrastructures Protection Act of 2001* (Ley de protección de infraestructuras críticas de 2001), Párrafo 5195c(e) del Título 42 del Código de EE. UU., (2001). También existe la definición de «activos o sistemas que son fundamentales para el mantenimiento de las funciones sociales, la salud, la seguridad y el bienestar social o económico de las personas». Consejo de la Unión Europea, *Directiva del Consejo 2008/114/CE del 8 de diciembre de 2008 sobre la Identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*, Diario Oficial de la Unión Europea, (8 de diciembre de 2008), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114.

43 Erik Brattberg y Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks,* (Interferencia en las elecciones rusas: la respuesta de Europa a las noticias falsas y los ciberataques) Fondo Carnegie para la Paz Internacional (23 de mayo de 2018), https://carn-egieendowment.org/2018/05/23/russian-election-int europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435. Véase también Michael McFaul, ed., *Securing American Elections* (La seguridad en las elecciones estadounidenses), Centro de Política Cibernética de Standford (junio de 2019), https://cyber.fsi.stanford. edu/securing-our-cyber-future.

44 Véase, por ejemplo, el documento del Departamento de Seguridad Nacional de los Estados Unidos, «Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector» (Declaración del Secretario Jeh Johnson sobre la designación de la infraestructura electoral como subsector de infraestructura crítica) (6 de enero de 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastruc-ture-critical.

propone un enfoque flexible y extensible que permita a los Estados y a otras partes interesadas adoptar algunas normas y al mismo tiempo rechazar o abstenerse de otras. Este enfoque no solo crea claridad al poner de relieve esferas concretas de acuerdo y desacuerdo, sino que permite que se adopten, perfeccionen y apliquen determinadas normas, aunque se necesite más tiempo para evaluar otras. En cualquier caso, la adopción generalizada de las normas será un esfuerzo a largo plazo.

También hay algunos desafíos únicos y prácticos a la hora de promover la adopción de normas. El desafío único es que estamos tratando de hacer frente a comportamientos relativamente nuevos y desestabilizadores. En la medida en que una norma es «algo usual, típico o estándar»,[45] la redacción de normas sobre el comportamiento futuro es un ejercicio interesante. Si todo el mundo ya se está comportando de cierta manera, entonces una norma escrita está simplemente codificando la práctica existente. Pero si no hay un «comportamiento típico», entonces redactar una norma es un intento de fomentar un comportamiento común en el futuro, incluso aunque no haya un comportamiento común en la actualidad. El simple hecho de declarar algo deseable no lo convierte en norma, por lo que es necesario promover su adopción.

En segundo lugar, es necesario que haya una mayor conciencia de las normas propuestas por las entidades capaces de aplicarlas, así como de las que las normas están concebidas para proteger. Incluso con una actividad significativa en las Naciones Unidas y en otros muchos foros, la adopción de normas se encuentra todavía en sus inicios y queda mucho por hacer para promover las normas propuestas y asegurar su aceptación, en particular en ciertas partes del mundo. Por ello, los esfuerzos por desarrollar capacidades en esta área son tan vitales; las organizaciones con mayor capacidad tienen más probabilidades de apoyar eficazmente la adopción de normas y conseguir más adhesiones es fundamental para cualquier estructura normativa mundial. Además, deben realizarse actividades de divulgación entre las personas protegidas por las normas, ya que es posible que no sean conscientes de sus posibles repercusiones. Por ejemplo, no parece haber una conciencia generalizada entre los Equipos de Respuesta a Emergencias Informáticas (CSIRT/CERT) sobre la norma del Grupo de Expertos Gubernamentales de las Naciones Unidas relativa a que los Estados no deben atacar a los CSIRT nacionales y utilizarlos solamente con fines defensivos. Tal y como se explica más adelante, las entidades protegidas tendrán a menudo un papel en la aplicación y la rendición de cuentas (así como en el diseño de la norma propuesta), pero no pueden cumplir esas funciones si no tienen conocimiento o información sobre las propuestas que hacen los actores estatales y no estatales. Es evidente que los gobiernos y las organizaciones internacionales deben hacer más para llegar a las comunidades a las que se pretende ayudar con las normas propuestas.

45 Consúltese https://www.lexico.com/en/definition/norm.

C. Aplicación de las normas

Tras la adopción, los actores estatales y no estatales deben tomar medidas concretas para aplicar una norma. Parece que existe un consenso creciente en los procesos en curso de las Naciones Unidas (OEWG y GGE) y en los esfuerzos regionales en el sentido de que la aplicación es una prioridad.[46] Para algunos, la aplicación se refiere a la adopción de la norma, la participación en esfuerzos de desarrollo de capacidades y medidas de fomento de la confianza, o el logro de un consenso más consistente sobre el significado de una norma acordada.[47] Si bien estas medidas son requisitos previos importantes para la aplicación de las normas, no sirven para aplicar las normas propiamente dichas. Por ejemplo, si bien el desarrollo de capacidades es necesario para garantizar que los países se puedan asegurar de disponer del ancho de banda necesario para participar a nivel internacional, se pueden desarrollar capacidades sin necesidad de adoptar o implementar normas. Del mismo modo, si bien las medidas de fomento de la confianza pueden contribuir a mantener la estabilidad del ciberespacio facilitando el intercambio de opiniones nacionales sobre la doctrina cibernética, organizando líneas telefónicas directas para la comunicación rápida entre los expertos nacionales en cibernética y fomentando el intercambio de prácticas recomendadas y normas de seguridad, estas también pueden llevarse a cabo sin necesidad de implementar normas. Más bien, implementar una norma implica tomar medidas concretas para dotarla de fuerza. A nivel nacional, esto podría incluir la

46 Resolución por la asamblea general 73/266, p. 3, párrafo 1(b), https://undocs.org/es/A/RES/73/266; Resolución por la asamblea general 73/27, p. 5, párrafo 5, https://undocs.org/es/A/%20RES/73/27. Véase también Organización para la Seguridad y la Cooperación en Europa (OSCE, por sus siglas en inglés), *Opening remarks by Secretary General Thomas Greminger* (Discurso de apertura del Secretario General Thomas Greminger), 2019 Presidencia de la Conferencia sobre la seguridad cibernética y de las TIC en toda la OSCE (Bratislava, 2019). «Las organizaciones regionales… pueden servir para incubar nuevas ideas y esfuerzos prácticos relacionados con CBM, así como para implantar acuerdos de aceptación a escala mundial, como por ejemplo los informes del Grupo de Expertos Gubernamentales. Por ello, las organizaciones regionales se dedican tanto a incubar como a implantar».

47 La Asamblea General de las Naciones Unidas invita a todos los Estados Miembros a que, teniendo en cuenta las evaluaciones y recomendaciones incluidas en los informes del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta, sigan comunicando al Secretario General sus opiniones y evaluaciones sobre, *entre otros*, «en el plano nacional para fortalecer la seguridad de la información y promover la cooperación internacional en esta esfera» y «las posibles medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial». Véase el informe del Secretario General de la ONU 74/120, https://undocs.org/es/A/74/120. Para consultar más opiniones a nivel nacional de los Estados miembros, véase https://www.un.org/disarmament/ict-security/.

incorporación de las normas propuestas a la política, la legislación y la doctrina militar nacionales. A nivel internacional, esto podría incluir el hecho de citar las disposiciones de una norma al atribuir los ataques o al adoptar medidas diplomáticas. Hacer operativa una norma de esta manera también sirve para darle una definición más precisa.

D. Rendición de cuentas

Una vez adoptadas y aplicadas las normas, debe haber una rendición de cuentas para quienes las infringen. Esto plantea las complicadas cuestiones de la atribución y la respuesta, que han demostrado ser difíciles de resolver en los ciberataques.

Para respaldar la afirmación de que un actor estatal o no estatal ha actuado de forma ilícita se requiere una atribución creíble. Esto empieza con la recogida y el análisis de pruebas, y se puede hacer ahora un trabajo tanto técnico como de procedimientos para mejorar la calidad y la puntualidad de la atribución. Más concretamente, al igual que en otras disciplinas técnicas, es importante disponer de protocolos bien aceptados para la recogida y el análisis de pruebas a fin de mejorar la calidad de las investigaciones. Así pues, la normalización de los métodos de investigación es importante porque puede reducir las preocupaciones sobre la integridad de las pruebas, incluso si la atribución debe decidirse caso por caso. Además de mejorar la atribución como un asunto técnico, es mucho lo que se puede hacer para acortar los procesos burocráticos relacionados con la toma de decisiones de atribución y luego, en el momento adecuado, hacerlas públicas. El lapso, a menudo prolongado, entre un acontecimiento y una declaración de responsabilidad se debe, en gran medida, a procesos poco claros o poco prácticos para adoptar esas decisiones a nivel nacional y esto se agrava cuando varios países participan en la formulación de declaraciones de atribución colectiva. El diseño y la puesta en práctica de procesos para alcanzar la atribución a nivel nacional e internacional, así como un mayor intercambio de información entre los países, pueden mejorar considerablemente la oportunidad y la eficacia de las declaraciones de atribución y facilitar cualquier otra medida apropiada.

Incluso después de que las pruebas apunten a un actor determinado, es posible que el siguiente paso (atribución) siga siendo un reto. En el pasado, algunos actores estatales y no estatales han afirmado que la atribución es imposible o que requiere una prueba definitiva. Pero no se requiere una prueba definitiva y, aunque la atribución puede resultar difícil, no es tan inalcanzable como algunos han sugerido. En el contexto del Estado nación, la atribución, ya sea en el ámbito cibernético o físico, suele ser un acto político, y aunque no existe un criterio de prueba acordado en particular, los países siguen teniendo un fuerte incentivo para no hacer acusaciones falsas, a fin de no perder credibilidad. En resumen, lo que se necesita es que la atribución sea convincente para otros países y para el público.

Incluso si una parte agraviada está convencida de que un determinado actor es responsable (y la atribución se ha producido de hecho en casos internacionales), conseguir que los actores rindan verdaderamente cuentas también ha resultado ser un reto, lo que ha debilitado el valor de las normas. Después de todo, si no hay consecuencias adversas para quienes infringen las normas aceptadas, esas normas se convierten en poco más que palabras sobre el papel y es poco probable que disuadan de llevar a cabo actividades desestabilizadoras.

La rendición de cuentas por los ataques cibernéticos perpetrados por actores no estatales es relativamente sencilla y se logra predominantemente por medio de la imposición de responsabilidad civil o penal en virtud de las leyes internas de los Estados interesados. No cabe duda de que se plantean problemas al respecto, ya que el carácter internacional de muchos ataques cibernéticos y las dificultades técnicas para reunir pruebas pueden obstaculizar la acción de los Estados. Sin embargo, el camino a seguir está conceptualmente claro: optimizar los procesos de aplicación de la ley a nivel internacional y trabajar para asegurar que los ciberdelincuentes sean identificados y procesados.

Hacer que los Estados rindan cuentas por las infracciones de las normas es más difícil.[48] Esto es debido a que la respuesta a un ataque en el ciberespacio depende en gran medida del contexto. En cuanto a si se exige o no la rendición de cuentas, los actores estatales y no estatales sopesarán diferentes factores; por ejemplo, un Estado que responda a una infracción de las normas puede considerar las repercusiones políticas, mientras que una empresa del sector privado puede considerar las repercusiones comerciales y de reputación. Por lo que respecta a la forma en que debe tratarse una infracción de las normas, las medidas estatales disponibles en respuesta a una infracción de las normas pueden considerarse a lo largo de un continuo, ya que la respuesta puede ser menor (por ejemplo, una denuncia privada), significativa (por ejemplo, sanciones económicas) o drástica (por ejemplo, una respuesta cinética muy visible). Si bien no hay ni habrá una respuesta única para todos los casos, es evidente que debe haber consecuencias significativas para las infracciones de las normas y el derecho internacional. Dado que los esfuerzos realizados en el pasado para hacer cumplir las normas han tenido un éxito limitado, se necesitan respuestas más eficaces y oportunas,

48 Es posible que se exija a los Estados responsabilidades por las operaciones cibernéticas que llevan a cabo, dirigen o autorizan. El principio de diligencia debida también puede resultar útil para definir el nivel de atención obligatoria para los Estados en el ciberespacio. Joanna Kulesza, *Due Diligence in International Law* (Diligencia debida en derecho internacional), (Leiden: Brill Nijhoff, 2016), https://doi.org/10.1163/9789004325197. Véase también, *Articles on Responsibility of States for Internationally Wrongful Acts* (Artículos sobre responsabilidad de los Estados por actos dolosos a escala internacional), aprobados por la Comisión de Derecho Internacional en su 53.º sesión, celebrada en 2001, adjunto a la resolución 56/83 de la Asamblea General, de 12 de diciembre de 2001, y corregido por el documento A/56/49(Vol I)/Corr4, artículos 4 y 11, http://legal.un.org/ilc/texts/instruments/draft_arti-cles/9_6_2001.pdf.

reconociendo que esas respuestas deben tratar de minimizar posibles inestabilidades futuras.

Los actores no estatales también están trabajando para garantizar que los infractores de las normas rindan cuentas de sus actos. Por ejemplo, el GFCE[49] reúne a miembros del gobierno, la sociedad civil y el sector privado para ayudar a coordinar los esfuerzos de desarrollo de capacidades, un requisito previo necesario para la adopción e implementación de normas y la rendición de cuentas. Además, el sector privado ha asumido un papel más amplio en la atribución de los ataques, utilizando tanto la información privada como pública para descubrir a los actores y describir los daños que han causado. Por último, algunas entidades del sector privado como el «CyberPeace Institute»,[50] han propuesto o puesto en marcha iniciativas encaminadas a supervisar y poner al descubierto grandes acontecimientos cibernéticos de manera más sistemática y a una escala potencialmente mayor.

Los actores no estatales deben desempeñar un papel más importante a la hora de hacer que los infractores rindan cuentas de sus transgresiones. La idea de aplicar normas por parte del sector privado no es nueva: por ejemplo, en 1977 durante la lucha contra el apartheid desarrollada en Sudáfrica, General Motors promovió una serie de principios de gran aceptación para llevar a cabo actividades empresariales (o no llevarlas a cabo) en dicho país; de este modo, más de 125 empresas extranjeras llegaron a retirar sus inversiones en el país.[51] En un caso más reciente, y de tono más simbólico, la respuesta de numerosas empresas (y administraciones) al asesinato por parte de Arabia Saudí del periodista opositor Jamal Khashoggi fue boicotear la Iniciativa de Inversión Futura como mensaje de desaprobación.[52] Este tipo de esfuerzos merecen ser examinados más a fondo.

E. Comunidades de intereses

Pese a que resulta fundamental desarrollar un modelo en el que participen múltiples agentes para la adopción e implantación de normas, así como para el establecimiento de responsabilidades, aprovechar las energías y capacidades de estos grupos plantea todo un reto. Las administraciones suelen utilizar el término «naciones afines» para reflejar la existencia de un grupo de Estados con ideas similares; no obstante, no existe un término equivalente que abarque un compendio de estados, empresas privadas, organizaciones sin ánimo de lucro (entre las que se incluyen las organizaciones normativas), la sociedad civil y particulares que compartan opiniones relacionadas con un aspecto específico. Esto es importante porque las normas propuestas por el Grupo de Expertos Gubernamentales de las Naciones Unidas y la Comisión Mundial sobre la Estabilidad del Ciberespacio pueden afectar a diferentes grupos, y es posible que ciertas organizaciones y miembros de la sociedad estén más interesados en promover algunas normas que otras. Como las administraciones, el sector privado, la comunidad técnica, el mundo académico y la sociedad civil no son entidades monolíticas, es importante reflexionar sobre la manera de crear un esfuerzo concertado, en lugar de concentrado, que integre diversas comunidades en aspectos relacionados con las normas.[53] La creación de Comunidades de intereses permite a aquellos que dispongan de competencias relativas a normas específicas trabajar en su desarrollo e implantación de forma más específica. Por ejemplo, los Equipos de Respuesta a Emergencias Informáticas (CERT/CSIRT, por sus siglas en inglés) pueden tener un especial interés en la implantación y supervisión de una norma del Grupo de Expertos Gubernamentales de las Naciones Unidas cuyo objetivo sea la protección de dicha comunidad, igual que los responsables de sistemas electorales pueden tener un interés especial en la norma de la Comisión Mundial sobre la Estabilidad del Ciberespacio relacionada con sistemas electorales. De forma similar, la comunidad de Internet podría ayudar a promover, aplicar y supervisar la norma propuesta por la Comisión sobre protección del núcleo público de Internet, mientras que los desarrolladores pueden estar más interesados en la norma relativa a la manipulación de productos.

La creación de una Comunidad de intereses puede estar dirigida o tratarse de un proceso constructivo ascendente establecido con fines específicos. El hecho de que los mismos miembros puedan establecer una Comunidad no sugiere que su desarrollo y éxito deba dejarse al azar. En su lugar, es importante centrarse en aquello que hace que una Comunidad se desarrolle de forma satisfactoria: (1) principios compartidos; (2) enfoque del tema; (3) competencias relacionadas; (4) apoyo financiero y administrativo y (5) transparencia en el proceso. De hecho, tal vez sea posible determinar un modelo de mejores prácticas sobre la forma en que deben crearse e implantarse las Comunidades, permitiendo así que diversos procesos de establecimiento de normas aprovechen un modelo comunitario similar. Esto ayudaría a conciliar las distintas líneas de trabajo para garantizar la eficiencia y el enfoque objetivo, así como a aprovechar las mejores prácticas para la adopción, implantación y rendición de cuentas de normas.

49 Foro Mundial sobre Conocimientos Cibernéticos, https://www.thegfce. com/.
50 Instituto CyberPeace, https://cyberpeaceinstitute.org/.
51 Véase, en general, «Sullivan Principles» (Principios de Sullivan), Wikipedia, 12 de agosto de 2018, https://en.wikipedia.org/wiki/Sullivan_principles.
52 Véase «Western boycott of Future Investment Initiative 2018», (Boicot occidental a la Iniciativa de Inversión Futura, 2018) *Royal News*, 16 de octubre de 2018, https://en.royanews.tv/news/15500/2018-10-16.
53 Véase, en general, *The Age of Digital Interdependence* (La era de la interdependencia digital), https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCo-operation-report-for-web.pdf.

7. RECOMENDACIONES

Nuestras seis recomendaciones para garantizar la estabilidad del ciberespacio se derivan de nuestros principios de responsabilidad, moderación, obligación de actuar y respeto de los derechos humanos. Dado que cada uno es responsable de garantizar la estabilidad del ciberespacio, siendo fundamental disponer de un modelo de múltiples partes interesadas, nuestras recomendaciones también tratan de aprovechar las capacidades de los actores estatales y no estatales, en parte a través de las Comunidades de intereses. En resumen, nos centramos en lo que se *debe* hacer y en cómo se *podría* llevar a cabo.

1. **Los actores estatales y no estatales deben adoptar y aplicar normas que mejoren la estabilidad del ciberespacio promoviendo la moderación y fomentando la acción.** Los actores estatales que hayan aceptado previamente las normas deben definir con mayor claridad los términos utilizados, resultado que podría lograrse a través de nuevas negociaciones y mediante la experiencia práctica de la aplicación de las normas existentes. Tanto los actores estatales como no estatales deben ofrecer pruebas claras relativas a la adopción e implantación de normas mediante declaraciones públicas y cambios tanto a nivel normativo como de actuación.

2. **Los actores estatales y no estatales, en consonancia con sus responsabilidades y limitaciones, deben responder adecuadamente a las infracciones de las normas, garantizando que aquellos que las infrinjan deban afrontar consecuencias previsibles y significativas.** El desarrollo e implantación de normas no será eficaz si aquellos que las infringen saben que no van a tener que pagar ningún precio por dichas infracciones. Por tanto, los actores estatales y no estatales deben desarrollar la capacidad interna de evaluar las infracciones y decidir y adoptar rápidamente respuestas individuales y colectivas oportunas, de conformidad con el Principio de Obligación de Actuar.

3. **Los actores estatales y no estatales, entre los que se incluyen las instituciones internacionales, deben redoblar sus esfuerzos por formar al personal, fomentar la capacidad y los medios, promover un conocimiento compartido de la importancia de la estabilidad del ciberespacio y tener en cuenta las diversas necesidades de las distintas partes.** La mejora de la capacidad, las competencias y los conocimientos servirá para ampliar la capacidad a escala mundial para aplicar leyes, normas y demás medidas internacionales de fomento de la confianza destinadas a mejorar la estabilidad del ciberespacio respetando los derechos humanos. Todas las partes deben aprovechar la existencia de organizaciones, entre las que se incluye el Foro Mundial sobre Conocimientos Cibernéticos en el que participan múltiples agentes, las cuales centran su actividad en el desarrollo de capacidades, ya que supone un requisito previo para la adopción y aplicación de normas, el establecimiento garantizado de responsabilidades, la adopción de otras medidas de estabilidad y el respeto de los derechos humanos.

4. **Los actores estatales y no estatales deben recopilar, compartir, estudiar y publicar información relacionada con infracciones de normas y el impacto resultante de dichas actividades.** Pese a que el mundo ha sido testigo de acciones que podrían suponer una infracción

de las normas establecidas en las Naciones Unidas y propuestas por la GCSC, la presentación de denuncias de esta situación tiende a ser anecdótica. Las organizaciones, sobre todo aquellas que son independientes de intereses comerciales o estatales, deben recopilar y publicar de forma sistemática información relacionada con infracción de normas y su impacto correspondiente. Esto servirá para catalizar las respuestas de actores estatales y no estatales a infracciones de las normas, así como para mejorar el cumplimiento de las mismas.

5. **Los actores estatales y no estatales deben establecer y prestar apoyo a las Comunidades de intereses para ayudar a garantizar la estabilidad del ciberespacio.** El establecimiento y apoyo a las Comunidades servirá para garantizar que todas las partes interesadas, incluidos los Estados, el sector privado, la comunidad técnica, el mundo académico y la sociedad civil, cumplan su responsabilidad de garantizar la estabilidad del ciberespacio. Estas Comunidades pueden centrar sus esfuerzos, entre otras cosas, en la interpretación, adopción e implantación de las normas de seguridad cibernética que se presentan en este informe y en otros documentos o publicaciones, independientemente de la solidez de las normas de presentación de pruebas de atribución, e independientemente de que los infractores de las normas sean responsabilizados de manera oportuna y eficaz.

6. **La GCSC recomienda establecer un mecanismo permanente de participación de múltiples partes interesadas para abordar cuestiones de estabilidad, en el que los Estados, el sector privado (incluida la comunidad técnica) y la sociedad civil participen y atiendan consultas de forma adecuada.** El Principio de responsabilidad reconoce que cada persona posee una función a la hora de garantizar la estabilidad del ciberespacio y refuerza la necesidad de establecer modelos de participación de múltiples partes interesadas. En el periodo comprendido entre 2011 y 2017, la Conferencia Mundial sobre el Ciberespacio (GCCS) constituyó una plataforma para dicha participación, llegando a atraer participantes pertenecientes a los Ministerios de Asuntos Exteriores y de Interior encargados de lograr la estabilidad mundial en otros contextos, además de ser el punto de partida del Foro Mundial sobre Conocimientos Cibernéticos, una importante herramienta para el desarrollo de capacidades. El Foro para la Gobernanza de Internet (FGI) también ha supuesto una importante plataforma para el debate entre múltiples agentes. Más recientemente, el Llamamiento de París ha conseguido reunir a la mayor comunidad multisectorial de partidarios del establecimiento de normas de seguridad cibernética de todos los tiempos. Estos esfuerzos sugieren que es el momento para desarrollar una comunidad mundial multisectorial, que sea inclusiva y orientada a desarrollar actuaciones cuyo objetivo sea la implantación práctica de las normas de ciberseguridad expuestas en este informe y en otras fuentes. Este mecanismo debe verse reforzado por una estructura permanente que asegure un esfuerzo continuo y sostenido.

APÉNDICE A: NORMAS ADOPTADAS POR EL GRUPO DE EXPERTOS GUBERNAMENTALES DE LAS NACIONES UNIDAS[54]

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 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;

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;

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;

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;

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;

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;

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;

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 A/70/174 15-12404 11/20 con las TIC originada en su territorio contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía;

i. Los Estados deberían adoptar las medidas pertinentes para garantizar l a 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;

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;

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.

54 Véase Asamblea General de las Naciones Unidas, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional)*, A/70/174 (22 de julio de 2015), https://undocs.org/es/A/70/174.

APÉNDICE B:
NORMAS DE LA GCSC

1. NO INTERFERENCIA CON EL NÚCLEO PÚBLICO

NORMA:

Los actores estatales y no estatales no deben llevar a cabo ni permitir a propósito actividades que perjudiquen intencional y sustancialmente la disponibilidad general o la integridad del núcleo público de Internet, y por tanto la estabilidad del ciberespacio.

ANTECEDENTES

La definición del núcleo público de Internet es un reto, ya que existen muchos tipos distintos de ataques que pueden, en última instancia, perjudicar la disponibilidad general o la integridad de Internet a gran escala (esta es la consecuencia que debe evitarse). Dicho esto, existen claramente ciertos componentes que deben establecerse como objetivo si se pretende ejercer un impacto de esta magnitud, siendo posible al menos aportar una lista no exhaustiva de dichos elementos críticos. En el nivel superior, la Comisión define la expresión «disponibilidad general» para indicar que la conducta de los actores ejerce un impacto sustancial en la población general. Por tanto, esta norma reconoce que aquellos Estados que la apoyan pueden seguir participando en actividades que estén más limitadas en objeto y alcance y que no ejerzan un impacto sustancial en la población general.

La Comisión define la expresión «el núcleo público de Internet» para referirse a aquellos elementos críticos de la infraestructura de Internet como pueden ser el encaminamiento y reenvío de paquetes, los sistemas de denominación y numeración, los mecanismos criptográficos de seguridad e identidad, los soportes de transmisión, el software y los centros de datos.

Entre los elementos de encaminamiento y reenvío de paquetes se incluyen, a título no limitativo, 1) los equipos, las instalaciones, la información, los protocolos y los sistemas que facilitan la transmisión de comunicaciones empaquetadas desde su origen a su destino 2) los Puntos de intercambio de Internet (los emplazamientos físicos donde se produce el ancho de banda de Internet); (3) los routers de núcleo e interpares de las principales redes que transportan dicho ancho de banda a los usuarios; (4) los sistemas necesarios para garantizar la autenticidad del encaminamiento y defender la red de comportamientos abusivos; (5) el diseño, la producción y la cadena de suministro de los equipos utilizados para los fines indicados anteriormente; y (6) la integridad de los propios protocolos de encaminamiento y sus procesos de desarrollo, normalización y mantenimiento.

Los sistemas de denominación y numeración incluyen, a título no limitativo, los siguientes: 1) los sistemas y la información utilizados en el funcionamiento del Sistema de Nombres de Dominio de Internet (incluidos los registros, los servidores de nombres, el contenido de zona, la infraestructura y los procesos como por ejemplo el DNSSEC utilizado para firmar criptográficamente los registros); 2) los servicios de información WHOIS para la zona raíz, la jerarquía de direcciones inversas, el código de país, los dominios de nivel superior geográficos e internacionalizados y para los nuevos dominios de nivel superior genéricos y no militares; 3) los resolvedores de DNS recursivos públicos de uso frecuente; 4) los sistemas de la Autoridad de Asignación de Números de Internet y los Registros Regionales de Internet que ponen a disposición y mantienen la asignación única de direcciones de Protocolo de Internet, Números de Sistema Autónomo e Identificadores de Protocolo de Internet; y 5) los propios protocolos de denominación y numeración y la integridad de los procesos y resultados de normalización para el desarrollo y mantenimiento de protocolos.

Entre los mecanismos criptográficos de seguridad e identidad se incluyen, a título no limitativo, los siguientes: 1) las claves criptográficas que se utilizan para autenticar usuarios y dispositivos y asegurar transacciones por Internet; 2) los equipos, las instalaciones, la información, los protocolos y los sistemas que permiten la producción, comunicación, uso y desaprobación de dichas claves; 3) los servidores de claves PGP, las Autoridades de Certificación y su Infraestructura de Claves Públicas; 4) DANE y sus protocolos e infraestructura de apoyo; 5) mecanismos de revocación de certificados y registros de transparencia; 6) administradores de contraseñas; 7) autenticadores de acceso itinerante; 8) mecanismos de tiempo exacto y establecimiento de precedencia temporal, como el Protocolo de Tiempo en Red y su infraestructura; 9) la integridad de los procesos y resultados de normalización del desarrollo y mantenimiento de algoritmos y protocolos criptográficos; y 10) el diseño, la producción y la cadena de suministro de los equipos utilizados para implantar procesos criptográficos.

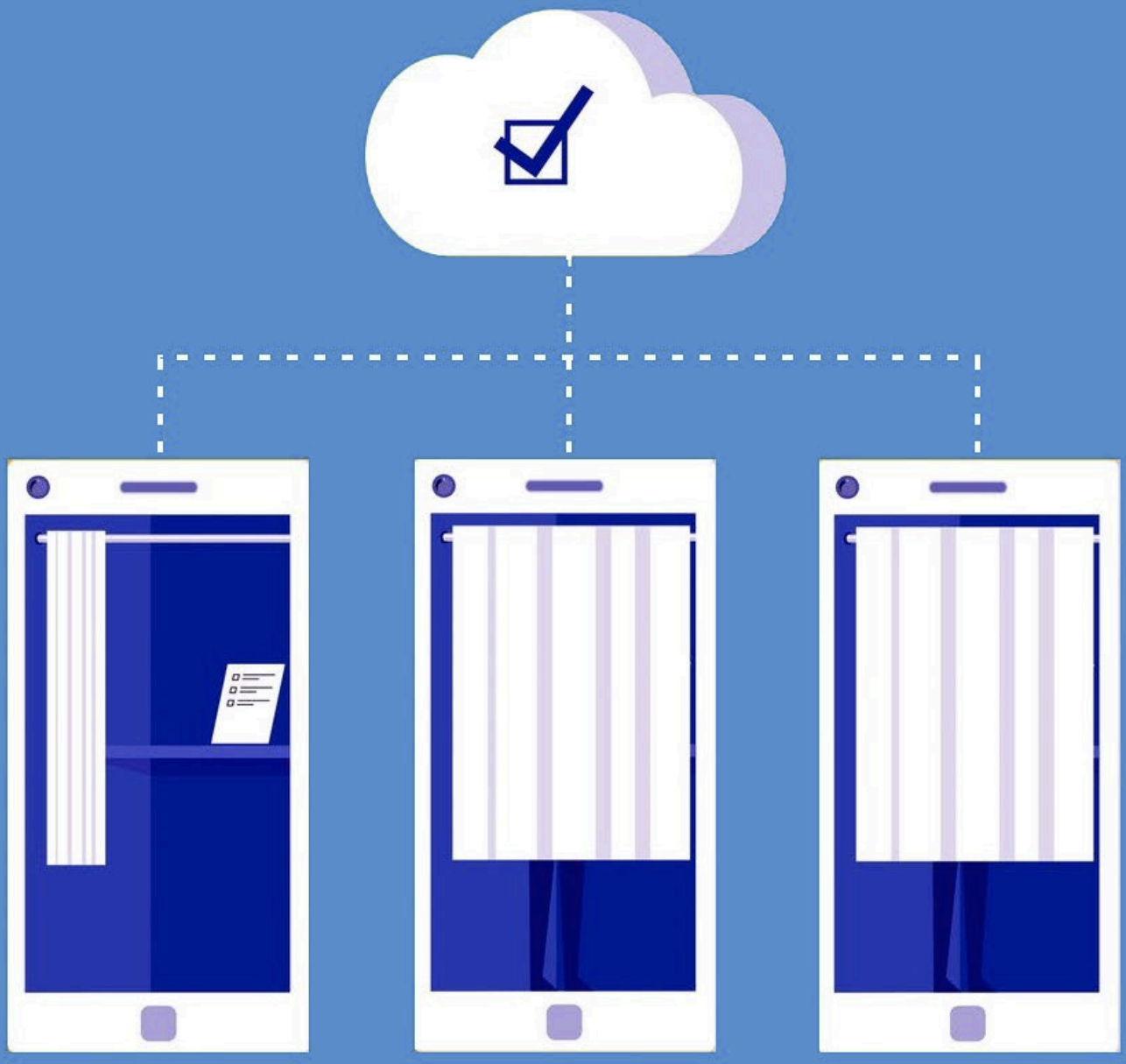
Los medios de transmisión incluyen, a título no limitativo, los siguientes: 1) la infraestructura, sistemas e instalaciones de comunicaciones que prestan servicios al público, ya sea por fibra, cobre o medios inalámbricos; 2) los cables terrestres y submarinos y las estaciones de desembarco, los centros de datos y demás instalaciones físicas que los sustentan; 3) las comunicaciones celulares y demás comunicaciones inalámbricas de voz y datos; 4) las comunicaciones de radiodifusión reguladas y no reguladas; 5) los sistemas de apoyo a la transmisión, regeneración de señal, ramificación, multiplexación y discriminación entre señal y ruido; y 6) los sistemas de cable que prestan servicios a regiones o poblaciones, pero no los que prestan servicios a los clientes de empresas individuales.

El software incluye, a título no limitativo, la disponibilidad e integridad de los procesos de desarrollo, el código fuente y la infraestructura de distribución de ajustes del software que se utiliza en el núcleo de Internet y por gran parte de los usuarios de Internet.

Los centros de datos incluyen a título no limitativo (1) las instalaciones físicas que albergan los servidores, contenidos e infraestructura de Internet; (2) el sistema utilizado para garantizar la seguridad de los centros de datos, la seguridad activa, el control de acceso físico, las operaciones, la gestión, el mantenimiento y los sistemas redundantes; y (3) los sistemas de comunicaciones utilizados para enviar comunicaciones a y desde centros de datos y en el interior de los mismos.

Los expertos consideran que son muchas más las categorías de infraestructura de Internet y de TIC que merecen protección, por lo que esta definición podría ampliarse en el futuro.

2. PROTECCIÓN DE LA INFRAESTRUCTURA ELECTORAL



NORMA:

Los actores estatales y no estatales no deben llevar a cabo, apoyar o permitir operaciones cibernéticas que tengan por objeto perturbar la infraestructura técnica esencial para la celebración de elecciones, referendos o plebiscitos.

ANTECEDENTES

De todas las normas, preceptos y principios que rigen la conducta de los Estados en la comunidad de naciones, la norma de no interferencia quizá sea la que se considere más valorada. El párrafo 4 del artículo 2 de la Carta de las Naciones Unidas articula esta norma y la eleva a principio de carácter jurídico y, por tanto, vinculante:

> Todos los Miembros, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o a cualquier otra forma incompatible con los Propósitos de las Naciones Unidas.

Mediante esta disposición, los redactores de la Carta reconocieron que las amenazas más graves al principio de no intervención provenían de medidas coercitivas dirigidas a la autonomía física o política de un Estado, ya que, de hecho, ambas son fundamentales para la soberanía de un Estado. El territorio controlado por un Estado puede ser una manifestación de su capacidad soberana; no obstante, no tiene valor alguno sin el disfrute de agencia e independencia política. Además, nada refleja la genuina independencia política más que los procesos de participación nacional, como por ejemplo unas elecciones que se desarrollen de forma libre y justa. El propósito de la Carta de las Naciones Unidas es conceder una protección sólida frente a interferencias externas indebidas. Dichas medidas de protección se han vuelto a cuestionar en la era digital.

Los expertos han debatido si el tipo de interferencia electoral relacionada con el ciberespacio que se ha visto recientemente equivale a una infracción ilícita de la soberanía (porque interfiere en el ejercicio de una función inherentemente gubernamental) o a una intervención ilícita.[55] No obstante, independientemente de que se haya producido o no una violación del derecho internacional, existe la clara posibilidad de que actores malintencionados, que actúen solos, colectivamente o en nombre de Estados, manipulen las elecciones utilizando medios digitales. Al hacerse más complejos los procesos de participación nacional tanto en escala como en sofisticación, se ha ampliado la cantidad de datos, instituciones e infraestructuras para su gestión. Muchos países publican hoy en día sus censos electorales en la red, una garantía básica y tradicional contra la manipulación de las votaciones o el fraude, exponiendo estas bases de datos a ataques cibernéticos y explotación. De forma parecida, los instrumentos de votación electoral se utilizan en zonas lejanas y remotas de un país, en las que sus operadores no son plenamente conscientes de los riesgos y dudas asociados a su manipulación digital. Los proveedores de software de votación y sistemas informáticos a nivel local o de «cabina» también siguen siendo susceptibles de tales intrusiones.

Consciente del creciente número e intensidad de las amenazas a los procesos participativos y reconociendo que dichos ataques son inaceptables, la GCSC recomienda la adopción de medidas nacionales más estrictas y una cooperación internacional eficaz para prever, eliminar y responder a las intrusiones cibernéticas contra la infraestructura técnica electoral. La Comisión reconoce que la celebración efectiva de elecciones o procesos participativos a nivel regional, local o federal es firme competencia de los Estados, y que debe llevarse a cabo de conformidad con sus respectivas leyes nacionales. No obstante, los ataques cibernéticos a su infraestructura electoral pueden venir desde más allá de sus fronteras, por lo que resulta necesario una resolución de cooperación multilateral. A medida que más países optan por digitalizar su maquinaria electoral, los riesgos y vulnerabilidades relacionados con dicha infraestructura se multiplican, al igual que la perspectiva de una operación cibernética importante y ofensiva. Así pues, las administraciones deben asumir el compromiso de abstenerse de participar en operaciones cibernéticas contra la infraestructura electoral de otro Estado. Al recomendar esta norma, la Comisión solamente afirma que la interferencia electoral es intolerable, independientemente de que se considere una infracción del derecho internacional o no.

55 Véase Michael N. Schmitt, «'Virtual' Dis-enfranchisement: Cyber Election Med-dling in the Grey Zones of International Law» (Anulación virtual de derechos: intromisión electoral cibernética en las áreas de indefinición del derecho internacional) *Chicago Journal of International Law*, Vol. 19, Núm. 1, y Nicholas Tsagourias, «Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace» (Ciberinterferencia electoral, autodeterminación y principio de no intervención en el ciberespacio), https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/.

3. NORMA PARA EVITAR LA MANIPULACIÓN

NORMA:

Los actores estatales y no estatales no deben manipular los productos y servicios en el desarrollo y la producción, ni permitir que se manipulen, si al hacerlo pueden menoscabar sustancialmente la estabilidad del ciberespacio.

ANTECEDENTES

En una norma centrada en la «No interferencia con el núcleo público de Internet», la GCSC exhortó a los actores estatales y no estatales a que no dañaran intencionada y sustancialmente la disponibilidad general o la integridad del núcleo público de Internet. Para apoyar esta norma, la Comisión ha observado la dependencia cada vez mayor de otras infraestructuras en una Internet estable y segura, además de las posibles consecuencias importantes de su interrupción. Mientras que la norma del núcleo público se centra en el «núcleo de Internet», los particulares y las organizaciones dependen en gran medida de determinados productos comerciales para llegar a dicho núcleo público y aprovechar la conectividad que proporciona. Como consecuencia de ello, la manipulación de componentes clave de productos informáticos de software y hardware (incluidos, a título no limitativo, sistemas operativos, sistemas de control industrial, conmutadores, enrutadores y otros equipos de red críticos, productos y normas criptográficas básicas, diseño de microchips y aplicaciones de consumo para usuarios finales de uso generalizado) puede igualmente privar a la sociedad de la capacidad de utilizar y aprovechar Internet de manera segura, y mermar en general la confianza en su buen funcionamiento. Pese a que dichos ataques suelen aparecer en las noticias, lo que recibe menos atención es el hecho de que se pueda producir un ataque incluso antes de que un producto o su actualización llegue al mercado. Por ejemplo, un producto puede ser objeto de ataques mediante la inserción de una vulnerabilidad, o mediante la eliminación secreta de una función de seguridad, en la fase de diseño y fabricación o durante la implantación de una de sus actualizaciones. Es decir, un producto puede ser manipulado con anterioridad a su lanzamiento o producción, con consecuencias para el público en general. El tiempo que transcurre entre la inserción de una vulnerabilidad y su activación para uso pernicioso puede variar.

Los Estados tienen intereses y responsabilidades que entran en conflicto cuando se trata de productos informáticos. Por otro lado, tienen la obligación de promover la resistencia e integridad de la infraestructura cibernética para ayudar a frustrar futuros ataques cibernéticos por parte de actores malintencionados y hacer que todo el ecosistema digital sea más seguro. Asimismo, los Estados tienen la obligación para sus ciudadanos de proteger la seguridad nacional y combatir la delincuencia y demás actores malintencionados que campan por el ciberespacio. Los Estados han explotado las vulnerabilidades de los productos y servicios digitales utilizados por sus adversarios para salvaguardar la seguridad nacional y pública. Así, en la medida en que los Estados consideren que la explotación de vulnerabilidades es un modelo eficaz para cumplir con sus responsabilidades, también pueden ver la utilidad de introducir intencionadamente debilidades o puertas traseras en los productos y servicios que utilizan sus adversarios. Los actores no estatales pueden, a su vez, manipular los productos y servicios, ya que sus objetivos pueden verse favorecidos por su capacidad para perturbar la estabilidad del ciberespacio. Merece la pena observar que la norma prohíbe manipular una línea de productos o servicios, ya que esto pone en riesgo la estabilidad del ciberespacio. Esta norma no prohibiría la adopción de medidas estatales selectivas que planteen escasos riesgos para la estabilidad general del ciberespacio; por ejemplo, la interceptación selectiva y la manipulación de un número limitado de dispositivos de usuario final para facilitar el espionaje militar o las investigaciones relacionadas con un delito. Este tipo de actividad, a no ser que se produzca dentro de la infraestructura básica del mismo núcleo público, o debilite de forma importante la confianza del usuario en Internet a nivel mundial, es poco probable que vaya a debilitar la confianza general en el ciberespacio, lo cual es una condición para la estabilidad cibernética. Pese a que los actores no estatales también pueden fijar sistemas como objetivo, dicha actividad podría infringir las leyes existentes en materia civil y penal.

Aunque los actores estatales y no estatales no deben manipular de manera expresa los productos en desarrollo o producción, los actores del sector también tienen la responsabilidad de impedir dichas actividades. Por consiguiente, los creadores de productos y servicios deben comprometerse a un nivel razonable de diligencia en el diseño, desarrollo y distribución de productos y servicios que dé prioridad a la seguridad y que, a su vez, reduzca la probabilidad, frecuencia, capacidad de explotación y gravedad de las vulnerabilidades. Las partes afectadas también deben rechazar toda acción estatal o no estatal que aparentemente ponga en peligro los productos y servicios, así como adoptar prácticas que reduzcan el riesgo de manipulación y les permitan responder si se descubre algún tipo de manipulación.

4. NORMA CONTRA LA INCAUTACIÓN DE DISPOSITIVOS DE TIC EN BOTNETS

NORMA:

Los actores estatales y no estatales no deben apropiarse de los recursos de las TIC de uso público para utilizarlos como redes de bots o con fines similares.

ANTECEDENTES

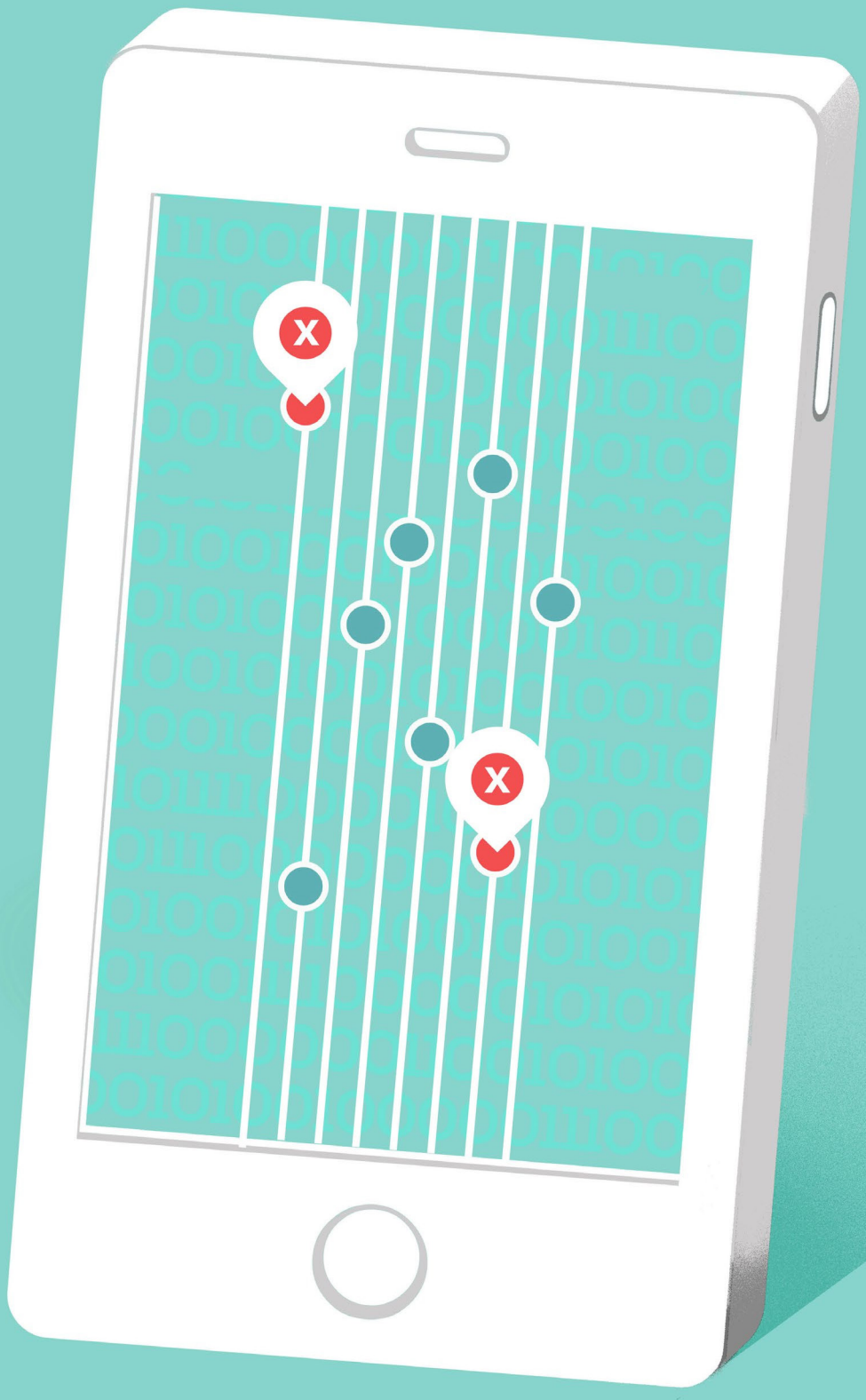
Los dispositivos con conexión a Internet están pasando a ser parte integrante del día a día de las personas en todas partes del mundo. Estamos rodeados de dispositivos con múltiples capacidades de computación, operativa en red, detección y actuación. Los termostatos, televisores, dispositivos médicos, despertadores y automóviles tienen capacidad de computación, almacenamiento y operativa en red que pueden ser incautados para hacer un mal uso de los mismos. El aprovechamiento de las vulnerabilidades en su código subyacente puede provocar problemas de seguridad física para las personas que utilicen el dispositivo: un dispositivo que funcione fuera de sus parámetros de diseño podría incendiarse o suponer un riesgo para la seguridad, como por ejemplo puertas que se abran inesperadamente, misiones de vídeo desde el interior de los hogares o provocar fallos en equipos (médicos).

Hablamos de botnets cuando se instalan agentes de software, en masa y sin consentimiento, para utilizar los recursos computacionales, de almacenamiento o de red de los dispositivos. Dichos botnets se pueden utilizar para ejercer un efecto directo en un sistema objetivo distinto, esto puede incluir la afectación en la confidencialidad, disponibilidad e integridad de los datos del objetivo final. Por tanto, un dispositivo de «terceros» que pudiera no tener nada que ver, y su propietario/operario, se convierten en parte de una actividad cibernética maliciosa sin saberlo. El riesgo que supone instalar agentes de software malicioso en dispositivos no solo es que se debilita la defensa del dispositivo frente a otros ataques, por ejemplo, de los delincuentes, o que infrinja el funcionamiento normal de estos, sino que también hace que el propietario/operario pueda considerarse culpable de los daños provocados al objetivo final. Es muy grave en aquellos casos en los que el dispositivo en riesgo pudiera hacer de forma inadvertida que su propietario/usuario actuase como parte beligerante involuntaria en hostilidades entre Estados, y por tanto incitar a que se produzcan represalias o deban asumirse responsabilidades.

A medida que dependemos cada vez más de la tecnología en nuestro entorno personal y entran en el mercado cada vez más dispositivos en conexión, la explotación de los dispositivos de consumo y su uso como botnets socava cada vez más la confianza y estabilidad de la sociedad. La Comisión reconoce que existen casos, por ejemplo, a efectos de aplicación de la ley, en que los actores estatales autorizados pueden considerar necesario instalar agentes de software en los dispositivos de un adversario o grupo de adversarios concreto. No obstante, los actores estatales y no estatales no deben incautar dispositivos civiles del público en general (en masa) para facilitar o ejecutar directamente operaciones cibernéticas ofensivas, independientemente de cuál sea el motivo.[56]

56 Esta norma es complementaria a la norma propuesta anteriormente para que los actores estatales y no estatales eviten manipular productos con anterioridad a su lanzamiento, la cual se centra en aspectos relacionados con la cadena de suministro, mientras que esta norma aborda aspectos relacionados con dispositivos ya en uso.

5. NORMA PARA QUE LOS ESTADOS CREEN UN PROCESO EQUITATIVO DE TRATAMIENTO DE VULNERABILIDADES



NORMA:

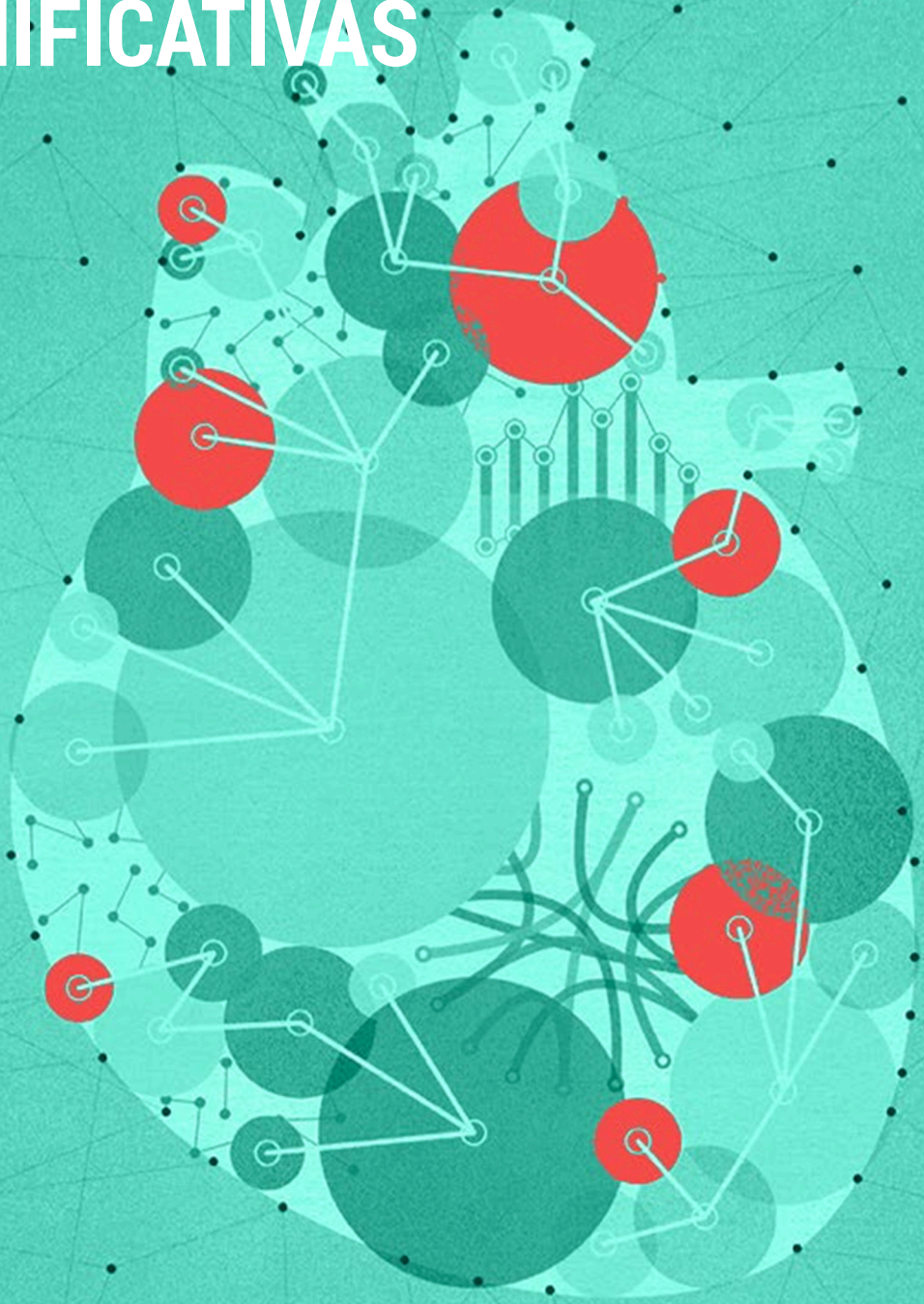
Los Estados deben crear marcos transparentes en materia de procedimientos para evaluar si deben revelar las vulnerabilidades o fallos no conocidos por el público en los sistemas y tecnologías de la información de los que tengan conocimiento, y cuándo deben hacerlo. De manera predeterminada se debe abogar por la divulgación.

ANTECEDENTES

A medida que crece la complejidad de los sistemas operativos, el software crítico y el hardware informático, sus vulnerabilidades son cada vez mayores. Dichas vulnerabilidades pueden ser aprovechadas por actores estatales o no estatales. Los Estados tienen en ocasiones intereses y responsabilidades que entran en conflicto cuando se trata de abordar vulnerabilidades de nueva aparición. Por un lado, tienen la obligación de promover la resistencia e integridad de la infraestructura fundamental para la estabilidad del ciberespacio ayudando a frustrar actividades cibernéticas malintencionadas y haciendo que todo el ecosistema digital sea más seguro para todos. Esto abogaría a favor de que los Estados revelen rápidamente las vulnerabilidades que acaben de descubrir a proveedores y fabricantes para el desarrollo de ajustes, y amplíen el ámbito de revelaciones públicas, cuando sea oportuno, para proteger al público en general. Por otro lado, los Estados tienen la obligación de proteger a sus ciudadanos de los delincuentes, investigar y enjuiciar los delitos cibernéticos, reservándose el derecho de imponer sanciones que actúen como medida disuasoria específica y general frente a futuras actividades malintencionadas. Una herramienta fundamental para perseguir a los actores malintencionados, y en particular a los más sofisticados, como pueden ser los Estados delincuentes, es la explotación de las vulnerabilidades de la infraestructura digital de la que dependen. Por tanto, los Estados a menudo sostienen que deben preservar al menos algunas capacidades escogidas, incluido el uso de vulnerabilidades no reveladas, o de lo contrario los actores malintencionados con grandes capacidades podrían pasar desapercibidos y no ser controlados.

Si bien es poco probable que los Estados revelen voluntariamente cada una de las vulnerabilidades que descubren, varios Estados han pasado recientemente de la presunción de que todas las vulnerabilidades se mantendrán sin revelar, a la presunción a favor de la revelación en aras de una mayor seguridad cibernética sistémica. Parte clave de ello es la creación, por parte de los Estados, de un proceso descrito abiertamente para evaluar los pros y los contras de efectuar revelaciones que tenga en cuenta todos los elementos de equidad normativa, económica, social y técnica. Más concretamente, dicho proceso debe ser transparente desde el punto de vista del procedimiento y tener en cuenta una amplia gama de opiniones que incluyan factores como por ejemplo la seguridad y la resistencia de la red, la seguridad de los usuarios y sus datos, el servicio de aplicación de la ley y la seguridad nacional, así como las repercusiones diplomáticas y comerciales. Los Estados Unidos han promulgado recientemente una nueva versión de dicho proceso y otros países están considerando la posibilidad de crear sus propias políticas de Proceso Equitativo de Vulnerabilidades (VEP, por sus siglas en inglés). Dado que la amplitud del descubrimiento y divulgación de vulnerabilidades trasciende las fronteras de cualquier Estado, a fin de promover la resistencia de la red y, al mismo tiempo, salvaguardar la seguridad nacional, redundaría en beneficio de la estabilidad a largo plazo del ciberespacio que todos los Estados dispusieran de este proceso. Además, los Estados deben trabajar para desarrollar procesos compatibles y previsibles. La existencia de dichos procesos puede actuar como medida de generación de confianza entre Estados, ya que aporta cierta seguridad que se contemplen plenamente los correspondientes elementos de equidad y los intereses en conflicto. Por supuesto, cada Estado tiene diferentes capacidades y estructuras interinstitucionales únicas; no obstante, cualquier proceso VEP eficaz debe diseñarse para tener en cuenta una amplia gama de perspectivas y elementos de equidad. Además, aunque las decisiones reales adoptadas en casos específicos pueden, por necesidad, seguir siendo confidenciales, debe existir transparencia en el marco y procedimientos generales para la adopción de dichas decisiones. Por último, esta norma trata exclusivamente el establecimiento de un proceso en el que se tomen decisiones relacionadas con divulgaciones. Si un gobierno o cualquier otra entidad decide hacer una divulgación, esta debe hacerse de una manera responsable que promueva la seguridad pública y no lleve a la explotación de dicha vulnerabilidad.

6. NORMA PARA REDUCIR Y ELIMINAR VULNERABILIDADES SIGNIFICATIVAS



NORMA:

Los productores y desarrolladores de productos y servicios de los que depende la estabilidad del ciberespacio deben: 1) dar prioridad a la seguridad y estabilidad, 2) adoptar medidas razonables para garantizar que sus productos o servicios estén libres de vulnerabilidades importantes, y 3) adoptar medidas para mitigar de forma oportuna las vulnerabilidades que se descubran posteriormente y para ser transparentes en cuanto a su proceso. Todos los actores tienen el deber de compartir información sobre las vulnerabilidades para ayudar a prevenir o mitigar las actividades cibernéticas malintencionadas.

ANTECEDENTES

Ciertos productos y servicios de tecnologías de la información son fundamentales para la estabilidad del ciberespacio debido a que se utilizan dentro de la infraestructura técnica básica, como por ejemplo en la resolución de nombres o encaminamiento básicos, porque facilitan ampliamente la experiencia del usuario en Internet, o porque se utilizan dentro de infraestructuras esenciales. Los creadores de productos y servicios deben comprometerse a un nivel razonable de diligencia en el diseño, desarrollo y distribución de productos y servicios que dé prioridad a la seguridad y que, a su vez, reduzca la probabilidad, frecuencia, capacidad de explotación y gravedad de las vulnerabilidades.

Debido a la complejidad cada vez mayor del software y el hardware, las vulnerabilidades de dichos productos constituyen una realidad. Si bien estas vulnerabilidades suelen ser involuntarias, los actores estatales y no estatales malintencionados se aprovechan a menudo de ellas cuando se descubren en formas que socavan la estabilidad del ciberespacio.

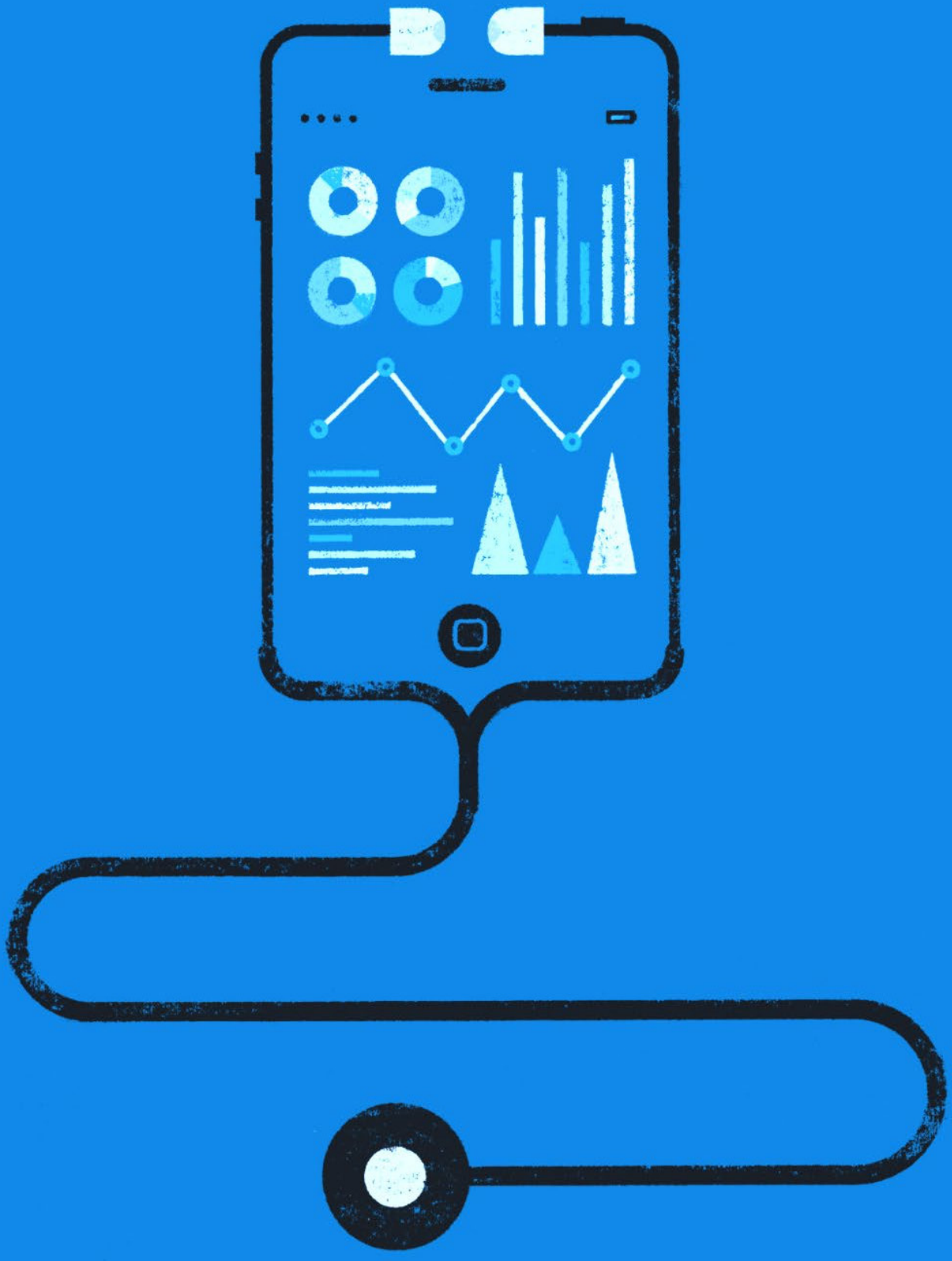
Además, en un mundo en que la conexión y la dependencia asumen una dimensión hiperbólica, el descubrimiento de una vulnerabilidad puede afectar a múltiples productos y servicios de distintos productores en entornos distintos. Llevar a cabo ajustes en un producto sin revelar a otros la vulnerabilidad subyacente puede proteger ese producto, pero no la estabilidad del ciberespacio a gran escala. Aquellos que se encuentran en la mejor posición para evaluar el impacto de una vulnerabilidad específica son a menudo los mismos que desarrollan, producen, instalan o utilizan productos afectados por las vulnerabilidades. Es importante compartir información que pudiera ayudar a solucionar vulnerabilidades de seguridad o que contribuya a evitar, limitar o eliminar un ataque.[57]

Aunque en la actualidad es muy difícil asegurar que no existan vulnerabilidades en los productos recién lanzados o actualizados, esta norma propuesta sugiere en cambio que quienes participan en el desarrollo o la producción de dichos productos adopten «medidas razonables» que reduzcan la frecuencia y la gravedad de las vulnerabilidades que se originen.

De la misma manera que la norma de «no manipulación» se refiere a la inserción intencionada de vulnerabilidades en productos y servicios fundamentales, y la norma de higiene se refiere en última instancia a los deberes de los usuarios finales, esta norma propuesta trata de que aquellos que desarrollan o producen productos esenciales tomen medidas razonables para garantizar que el número y el alcance de las vulnerabilidades críticas se reduzcan al mínimo y que se eliminen de manera eficaz y oportuna y, cuando proceda, se divulguen al ser descubiertas. El proceso utilizado debe ser transparente para crear un entorno previsible y estable.

57 Una de las normas de comportamiento responsable de los Estados en el informe de 2015 del Grupo de Expertos Gubernamentales de las Naciones Unidas (A/70/174) afirma que «los Estados deben fomentar la presentación responsable de informes sobre vulnerabilidades de las TIC y compartir la información relacionada sobre las soluciones disponibles para dichas vulnerabilidades a fin de limitar y posiblemente eliminar las potenciales amenazas a las TIC y a la infraestructura que depende de ellas».

7. NORMA SOBRE HIGIENE CIBERNÉTICA BÁSICA COMO DEFENSA FUNDAMENTAL



NORMA:

Los Estados deben promulgar medidas adecuadas, incluyendo leyes y reglamentos, para garantizar una higiene cibernética básica.

ANTECEDENTES

Al aumentar la conectividad de Internet en todo el mundo, ocupando todos los aspectos de la vida moderna, los usuarios de todo tipo (particulares, organizaciones, empresas y administraciones) se vuelven cada vez más dependientes de la tecnología y del acceso a la información disponible en Internet. La política, la economía, la información pública, la educación, el desarrollo y cualquier otra forma de interacción social dependen de manera fundamental de Internet y las tecnologías relacionadas. No obstante, esta maravilla moderna sigue siendo muy insegura, por lo que nadie es inmune a sus peligros.

Todavía tiene que surgir un consenso para encontrar las formas más eficaces de optimizar las prometedoras tecnologías del ciberespacio protegiendo a su vez al público en general. No obstante, la mayoría está de acuerdo en que las ventajas de nuestra vida en conexión digital no pueden sostenerse en su avance sin normas aceptadas de seguridad fundamental en el ciberespacio. A tal fin, la Comisión apoya firmemente la adopción generalizada y la implantación verificada de medidas de higiene cibernética básica, un régimen de medidas fundamentales que representen tareas básicas y prioritarias de defensa, prevención y eliminación rápida de peligros en el ciberespacio que pueden evitarse. De hecho, dada la extensión de la interconexión en línea, estas medidas constituyen una obligación básica de atención que debe exigirse a todos los usuarios. Los regímenes de higiene deben incorporar medidas fiables de implantación, aportar intercambio generalizado de información técnica y prácticas recomendadas, y ser objeto de supervisión oportuna. Los dispositivos y procesos inteligentes cada vez exigen más leyes y reglamentos inteligentes. Para crear más responsabilidad relacionada con esta obligación básica de atención cibernética, las administraciones no deben recortar la innovación ni modificar las propiedades básicas de Internet.

Ya existen normas de higiene cibernética en diversas formas.[58] Han alcanzado una mayor aceptación internacional, ya que las administraciones y empresas son cada vez más conscientes de la importancia de tomar medidas que hayan demostrado su utilidad para ayudar a evitar y eliminar con rapidez los peligros que conlleva el software malicioso conocido. Además, estas normas son representativas de las prácticas recomendadas, destacan la importancia de una supervisión habitual y razonable y resaltan la importancia del intercambio automatizado de información cuando sea posible para alertar a otros usuarios de la existencia de problemas. Dichas defensas cibernéticas básicas descritas en estos modelos justifican la realidad de que ningún gobierno, organización o grupo de usuarios puede mitigar de forma individualizada todos los riesgos cibernéticos. También reconocen que los usuarios de cualquier nivel desempeñan funciones importantes de fortalecimiento de la seguridad cibernética.

La GCSC cree que la defensa fundamental de la seguridad cibernética mediante la adopción generalizada de higiene cibernética ha pasado a ser fundamental para el uso responsable y el crecimiento ventajoso de Internet. La seguridad debe considerarse como un proceso continuo en el que las responsabilidades se distribuyan entre todos los actores que dispongan de mecanismos de presentación de informes automatizados o intercambio de información, entre otros, para garantizar una adecuada asunción de responsabilidades.

La Comisión reconoce también que muchas sociedades de todo el mundo se enfrentan a retos considerables en la utilización de las tecnologías de la información y la comunicación, y exhorta a los Estados a que compartan sus conocimientos y ofrezcan la creación de capacidades para instanciar procesos de aplicación efectiva de regímenes básicos de higiene cibernética a fin de ampliar el efecto de esta norma.

58 Esto incluye, por ejemplo, las del Instituto Europeo de Normas de Telecomunicaciones (ETSI, por sus siglas en inglés), el Centro de Seguridad de Internet (CIS, por sus siglas en inglés) sin ánimo de lucro, o la Dirección Australiana de Señales (ASD, por sus siglas en inglés), entre otros.

8. NORMA CONTRA OPERACIONES CIBERNÉTICAS OFENSIVAS POR PARTE DE ACTORES NO ESTATALES

NORMA:

Los actores no estatales no deben participar en operaciones cibernéticas ofensivas y los actores estatales deben prevenir dichas actividades y actuar en caso de que se produzcan.

ANTECEDENTES

Pese a que las Tecnologías de la Información y las Comunicaciones han transformado las sociedades en positivo, también plantean nuevos problemas de seguridad. La velocidad y ubicuidad de las operaciones cibernéticas plantean a menudo dificultades a los sistemas judiciales de los Estados y a la cooperación a la hora de hacer cumplir las leyes a escala internacional. A pesar de la existencia de estas dificultades, debe recordarse que la soberanía de los Estados es la piedra angular del sistema internacional de normas para la paz y la seguridad. Los Estados poseen el monopolio del uso legítimo de la fuerza, estrictamente limitado por el derecho internacional. Algunos actores no estatales, sobre todo empresas privadas, defienden el derecho a realizar operaciones cibernéticas ofensivas más allá de las fronteras nacionales, alegando potencialmente que constituyen una medida defensiva necesaria, ya que los Estados no tienen la capacidad de protegerlos adecuadamente contra las amenazas cibernéticas. Existe el eufemismo de llamar «defensa cibernética activa» a estas operaciones cibernéticas ofensivas desarrolladas por actores no estatales,[59] entre las que se incluyen, a título no limitativo, el denominado «contraataque informático», ya que se llevan a cabo como defensa.

Algunos Estados no controlan o, posiblemente, pasan por alto dichas prácticas, pese al riesgo que suponen para la estabilidad y la seguridad del ciberespacio. No obstante, en numerosos Estados dichas prácticas serían ilícitas, si no penalizadas, mientras que en otros no parecen estar prohibidas ni autorizadas explícitamente. Algunos Estados, no obstante, están considerando legitimar las operaciones cibernéticas ofensivas de actores no estatales. De hecho, algunos han decidido aprobar o han propuesto leyes internas para permitir el desarrollo de operaciones ofensivas por parte de actores no estatales.

La GCSC opina que dichas prácticas socavan la estabilidad del ciberespacio. Pueden provocar graves interrupciones y daños, incluidos daños a terceros, por lo que existe la posibilidad de que den paso a complejas disputas legales y a una escalada de conflictos. Los Estados que explícitamente concedan o den de forma intencionada a actores no estatales autorización para realizar operaciones ofensivas, para sus propios fines o los de terceros, podrían sentar un peligroso precedente y correrían el riesgo de infringir el derecho internacional. La Comisión cree que las medidas ofensivas deben reservarse exclusivamente a los Estados y recuerda que el derecho internacional establece un estricto marco exclusivo de respuestas de los Estados a hostilidades que también se aplica a las operaciones cibernéticas. De forma similar, según el derecho internacional, los actores no estatales que actúen en nombre de los Estados deben ser considerados sus agentes y, por tanto, extensiones del Estado.[60]

Si los Estados permiten dichas actuaciones, pueden por tanto ser considerados responsables según el derecho internacional.[61] Los Estados deben actuar, a nivel nacional e internacional, para evitar el desarrollo de operaciones cibernéticas ofensivas por parte de actores no estatales.

59 La defensa cibernética activa debe entenderse como una serie de medidas que abarcan desde la autodefensa en la red de la víctima a las actividades de destrucción de la red del atacante. Para el defensor, las operaciones cibernéticas ofensivas dentro de este continuo implican actuar fuera de su propia red, independientemente de su intención (ofensiva o defensiva) y la calificación legal de sus actos. Deben llevarse a cabo nuevos trabajos de definición de operaciones cibernéticas ofensivas y defensa cibernética activa.

60 Véase la «nota adicional» para un tratamiento más amplio del caso dentro del derecho internacional, la cual está disponible aquí: https://cybersta-bility.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf.

61 Id.

APÉNDICE C: HISTORIAL, OBJETIVOS Y PROCESOS DE LA GCSC

Desde su puesta en marcha en la Conferencia de Seguridad de Múnich de febrero de 2017, bajo el patrocinio del Ministro de Asuntos Exteriores de los Países Bajos, Bert Koenders, la Comisión Mundial sobre la Estabilidad del Ciberespacio ha sido considerada una de las primeras iniciativas de múltiples partes interesadas de este tipo que se concentran específicamente en la estabilidad del ciberespacio. Presidida por Michael Chertoff, ex Secretario de Seguridad Interior de Estados Unidos; Latha Reddy, ex Asesora Adjunta de Seguridad Nacional de la India; y anteriormente por Marina Kaljurand, Miembro del Parlamento Europeo y ex Ministra de Asuntos Exteriores de Estonia, la Comisión está integrada por 28 personas destacadas procedentes de diversas regiones geográficas y con distintos antecedentes relacionados con la seguridad cibernética internacional.[62] Cuenta con el apoyo de asesores especiales, una secretaría integrada por el Centro de Estudios Estratégicos de *La Haya* y el EastWest Institute, un Grupo Asesor de Investigación, y varios socios y patrocinadores, entre ellos el Ministerio de Relaciones Exteriores de los Países Bajos y Francia, el Organismo de Seguridad Cibernética de Singapur, Microsoft, la Internet Society y Afilias.

La Comisión nació del deseo de continuar la labor de anteriores comisiones de la sociedad civil, incluida la Comisión Mundial sobre la Gobernanza de Internet, y de cooperar con la Conferencia Mundial sobre el Ciberespacio (GCCS). En 2015, se pidió al Centro de Estudios Estratégicos de *La Haya* (HCSS, por sus siglas en inglés) que organizara una sesión preparatoria para la reunión de La Haya de la GCCS, dedicada a la paz y seguridad internacionales. Gran parte de la declaración posterior de la GCCS se basa directamente en el trabajo de la reunión preparatoria, en la que se subraya claramente la necesidad de un formato de múltiples partes interesadas para examinar las cuestiones relacionadas con la seguridad cibernética internacional. Por consiguiente, el HCSS convocó a un grupo básico de promotores y patrocinadores (en principio Microsoft, la Internet Society y el Ministerio de Asuntos Exteriores de los Países Bajos) y elaboró un plan estratégico. En agosto de 2016, tras haber conseguido que el EastWest Institute (EWI) se asociara a la Secretaría, el HCSS convocó una reunión del Grupo de Creación de la GCSC en la Harvard Kennedy School, en la que se redactaron los principales requisitos para el funcionamiento de la GCSC, su composición, estructura y objetivos, así como su declaración de objetivos.

La declaración de objetivos establece lo siguiente:

> La Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC, por sus siglas en inglés) elaborará propuestas de normas y políticas para mejorar la seguridad y la estabilidad internacionales y servir de guía para un comportamiento estatal y no estatal responsable en el ciberespacio. La GCSC animará a todas las partes interesadas a desarrollar ideas comunes, estando su trabajo dirigido a anticipar la estabilidad cibernética mediante el apoyo a la investigación, el intercambio de información y el desarrollo de capacidades.

Desde sus inicios, la GCSC pretendía influir en la agenda de paz y seguridad internacional relacionada con el ciberespacio, lo que por lo general se conoce como

62 Véase la lista completa de Comisionados en la página 4.

«ciberseguridad internacional.» El Grupo de Creación ha identificado una necesidad de solicitar ideas distintas, sobre todo de las comunidades técnicas y de gestión directiva de Internet, con respecto al debate continuo sobre seguridad cibernética internacional. El objetivo consiste en aportar mejor información a las deliberaciones de las comunidades sobre control de armas y de paz y seguridad, en las que gran parte del buen trabajo desarrollado, sobre todo en cuanto a normas, se considera obstaculizado por la falta de aportaciones y aceptación de estos actores de la sociedad civil y el sector privado. Por consiguiente, se consideró que el modelo de múltiples partes interesadas es una cuestión práctica más que ideológica.

El modelo adoptado por la GCSC para abordar sus deliberaciones presenta un enfoque «ascendente-descendente». En primer lugar, identificó normas operativas que satisficieran las necesidades de seguridad cibernética internacional más perentorias indicadas por sus miembros y que no hubieran sido atendidas por ninguna otra institución. En segundo lugar, extrapoló de estas normas y de otras ya existentes una definición operativa de estabilidad cibernética y sus principios subyacentes. En tercer lugar, se desarrolló un marco de estabilidad para comprender con mayor claridad cuáles son las características que la arquitectura de paz y seguridad internacionales debe poseer para cumplir dicha definición. Por último, desarrolló recomendaciones para agentes estatales y no estatales relacionadas con la forma en que podría llevarse a cabo este trabajo.

Las deliberaciones de los Comisionados para alcanzar dichos objetivos se han desarrollado sin fronteras geográficas y entre grupos de interesados. Desde el principio, la Comisión ha hecho hincapié en celebrar sus reuniones de forma paralela a las conferencias pertinentes para facilitar aportaciones de más partes interesadas.[63] También solicita de forma activa aportaciones derivadas de investigaciones y del trabajo de la comunidad en general. Para relacionar el trabajo de la GCSC con la comunidad académica en general, se ha puesto en marcha el Grupo Asesor de Investigación con un presidente y cuatro adjuntos a presidencia[64] responsables de administrar una lista de correo electrónico de más de 200 expertos. También ha sido la base de un amplio programa de investigación, que finalmente ha llegado a encargar más de 20 estudios a instituciones de investigación y particulares de todo el mundo.[65] La mayor parte de este trabajo fue presentado directamente a los Comisionados en las «Conferencias de Estabilidad Cibernética».

Antes de la publicación del presente informe y de las normas de publicación previa, la Comisión recabó sistemáticamente las aportaciones de numerosos agentes de la administración, la sociedad civil y la industria. Al escalonar la presentación de resultados a lo largo de todo el mandato de la Comisión, fue posible efectuar invitaciones constantes a la presentación de ideas y comentarios externos. Se publicaron Solicitudes de consultas en línea relacionadas con las normas de la GCSC y la definición de estabilidad cibernética. Se recibieron más de 23 trabajos de actores de todo el mundo, los cuales sirvieron como elementos de información para las deliberaciones de los Comisionados. Además, la Comisión participó activamente en más de 70 conferencias y actos, convocando mesas redondas, actos paralelos y debates dedicados a la estabilidad cibernética con numerosas partes interesadas estatales y no estatales.

Por último, los mismos Comisionados mantienen vínculos activos con sus respectivas comunidades. Las aportaciones e ideas de estos grupos representan la base de las interacciones con la comunidad general de expertos estatales y no estatales, y constituyen el fundamento de promoción del informe en el futuro.

63 Se convocaron reuniones oficiales de la Comisión en los siguientes eventos: Conferencia de Seguridad de Múnich de 2017 (Múnich, Alemania); CyCon (Tallin, Estonia); BlackHat USA (Las Vegas, EE. UU.); Conferencia Mundial sobre el Ciberespacio (Nueva Delhi, India); Foro Internacional de Ciberseguridad de la FIC de 2018 (Lille, Francia); Conferencia de Seguridad de Múnich de 2018 (Múnich, Alemania - Delegación); GLOBSEC (Bratislava, Eslovaquia); Semana Cibernética de Israel (Tel Aviv, Israel - Delegación); Semana Cibernética Internacional de Singapur (Singapur); Foro de la Paz y FGI de París (París, Francia - Delegación); Instituto de las Naciones Unidas de Investigación sobre el Desarme, 2019 (Ginebra, Suiza); Foro de la Comunidad ICANN 64 (Kobe, Japón); EuroDIG (La Haya, Países Bajos); Reunión Anual del GFCE (Addis Abeba, Etiopía).

64 Abarca cuatro áreas temáticas, entre ellas la paz y la seguridad internacionales, el derecho internacional, la gobernanza de Internet y la tecnología.

65 Véase la sección de Agradecimientos.

AGRADECIMIENTOS

La Comisión Mundial sobre la Estabilidad del Ciberespacio (GCSC) desea agradecer a las numerosas instituciones y personas que apoyaron, contribuyeron y facilitaron la labor de la Comisión, incluidos, a título no limitativo, nuestros patrocinadores, el Grupo Asesor de Investigación, los autores de los documentos de investigación y los revisores externos, así como el personal de apoyo. A continuación figuran algunos de los que contribuyeron al éxito de la Comisión.

Secretariado

CENTRO DE ESTUDIOS ESTRATÉGICOS DE *LA HAYA* (HCSS, POR SUS SIGLAS EN INGLÉS)

Alexander Klimburg, Director, Iniciativa y Secretaría de la Comisión Mundial sobre la Estabilidad del Ciberespacio
Louk Faesen, Director de proyectos, Secretaría de la Comisión Mundial sobre la Estabilidad del Ciberespacio
Elliot Mayhew, Auxiliar de proyectos, Secretaría de la Comisión Mundial sobre la Estabilidad del Ciberespacio

Con la colaboración adicional de: **Timon Domela Nieuwenhuis Nyegaard**, **Koen van den Dool**, **Niels Renssen** y **Kaja Karlson**.

EASTWEST INSTITUTE (EWI)

Elliot Mayhew, Codirector, Secretaría de la Comisión Mundial sobre la Estabilidad del Ciberespacio
Anneleen Roggeman, Director de proyectos, Secretaría de la Comisión Mundial sobre la Estabilidad del Ciberespacio

Con la colaboración adicional de: **Abagail Lawson**, **Dragan Stojanovski** y **Conrad Jarzebowski**.

Socios, patrocinadores y promotores

El Centro de Estudios Estratégicos de *La Haya*, el EastWest Institute y los Comisionados desean reconocer y agradecer el apoyo de las siguientes organizaciones:

COLABORADORES:

- **Ministerio de Asuntos Exteriores de los Países Bajos**, **Timo Koster** y **Dimitri Vogelaar**
- **Microsoft**, **Jan Neutze** y **Kaja Ciglic**
- **Agencia de Seguridad Cibernética de Singapur**, **David Koh** y **Sithuraj Ponraj**
- **Internet Society (ISOC)**
- **Ministerio de Asuntos Exteriores de Francia**, **Henry Verdier** y **David Martinon**
- **Afilias**, **Ram Mohan** y **Philipp Grabensee**

PATROCINADORES:

- **Departamento Federal de Asuntos Exteriores de Suiza**
- **GLOBSEC**
- **Ministerio de Asuntos Exteriores de Estonia**
- **Ministerio del Interior y Comunicaciones de Japón**

PROMOTORES:

- **Comisión de la Unión Africana**
- **Black Hat USA**
- **DEF CON**
- **Delegación de la Unión Europea ante las Naciones Unidas en Ginebra**
- **Foro Mundial sobre Conocimientos Cibernéticos**
- **Google**
- **Municipio de La Haya**
- **Packet Clearing House**
- **Universidad de Tel Aviv**
- **Instituto de las Naciones Unidas para el Desarme**

Estas organizaciones e instituciones están comprometidas con el avance del debate y con la propuesta de soluciones creativas para algunos de los retos más apremiantes a los que se enfrenta la estabilidad del ciberespacio.

Investigadores

La Comisión desea agradecer a los miembros de su Grupo Asesor de Investigación, un grupo de más de 200 miembros en línea que han conseguido establecer la conexión entre la GCSC y la comunidad académica en general. Sobre todo, no gustaría agradecer a los investigadores encargados de redactar informes y memorias informativas para la deliberaciones de los Comisionados.

INFORME 1 PUBLICADO POR LA GCSC (NOVIEMBRE DE 2017)

Alex Grigsby, anteriormente miembro del Consejo de Relaciones Exteriores (CFR, por sus siglas en inglés)
Deborah Housen-Couriel, Konfidas Digital Ltd.
Joanna Kulesza, Universidad de Lodz y **Rolf H. Weber**, Universidad de Zúrich
Oluwafemi Osho, **Joseph A. Ojeniyi** y **Shafi'i M. Abdulhamid**, Universidad Federal de Tecnología, Minna
Analía Aspis, , Universidad de Buenos Aires
Robert Morgus, anteriormente miembro de New America, **Max Smeets**, anteriormente miembro del Centro de de Seguridad y Cooperación Internacional de la Universidad de Stanford, y **Trey Herr**, Harvard Kennedy School
Arun Mohan Sukumar, **Madhulika Srikumar** y **Bedavyasa Mohanty**, Fundación de Investigación Observadora (ORF, por sus siglas en inglés)

INFORME 2 PUBLICADO POR LA GCSC (MAYO DE 2018)

Shen Yi, **Jiang Tianjiao** y **Wang Lei**, Centro de Investigación para la Gobernanza del Ciberespacio de la Universidad de Fudan
Elana Broitman, **Mailyn Fidler** y **Robert Morgus**, anteriormente miembro de New America
Elonnai Hickok y **Arindrajit Basu**, Centro para Internet y la Sociedad
Thomas Uren, **Bart Hogeveen** y **Fergus Hanson**, Instituto Australiano de Política Estratégica (ASPI, por sus siglas en inglés)
Dragan Mladenović y **Vladimir Radunović**, DiploFoundation
Thomas Reinhold, Instituto de Investigación sobre la Paz y la Política de Seguridad de la Universidad de Hamburgo

Consultas

La Comisión desea dar las gracias a las siguientes personas y organizaciones por haber presentado amplias observaciones en respuesta a la solicitud de consultas sobre el Conjunto de Normas de Singapur (del 17 de diciembre de 2018 al 17 de enero de 2019) y la definición de estabilidad del ciberespacio (del 14 de agosto de 2019 al 6 de septiembre de 2019):

Hussein Abul-Enein, Access Partnership
Kayode Akanni, DesignIT
Jonathan D. Aronson, Universidad del Sur de California (USC, por sus siglas en inglés)
Aviram Atzaba, Dirección Nacional de Cibernética de Israel
Arindrajit Basu, **Gurshabad Grover**, **Elonnai Hickok** y **Karan Saini**, Centro para Internet y la Sociedad
Vytautas Butrimas, Centro de Excelencia de Seguridad Energética de la OTAN
Cybersecurity Tech Accord
Michael Daniel, Alianza contra la Amenaza Cibernética
Global Partners Digital
Arvind Gupta y **Dickey Kumar**, Fundación Internacional Vivekananda
Tara Hairston y **Anastasiya Kazakova**, Kaspersky
Sven Herpig, Stiftung Neue Verantwortung
Drew Mitnick, Access Now
George M. Moore, Centro James Martin de Estudios de No Proliferación
Brett van Niekerk y **Trishana Ramluckan**, Universidad de KwaZulu-Natal
Peter Swire, **Justin Hemmings** y **Sreenidhi Srinivasan**, Escuela de Negocios de Georgia Tech Scheller
Johan de Wit, Siemens/TU Delft

Por último, la Comisión desea dar las gracias a los siguientes expertos, cuya labor y conocimientos especializados han orientado e informado las deliberaciones de la Comisión:

Dennis Broeders, Universidad de Leiden
Deborah Brown y **Verónica Ferrari**, Asociación para el Progreso de las Comunicaciones
Michael Daniel, Alianza contra la Amenaza Cibernética
François Delerue, Institut de Recherche Stratégique de l'École Militaire – IRSEM
Akhil Deo y **Arun Mohan Sukumar**, Fundación de Investigación de Observadores (ORF, por sus siglas en inglés)
Martha Finnemore, Universidad George Washington
Aude Géry, Universidad de Rouen
Duncan Hollis, Facultad de derecho de Temple
Joanna Kulesza, Universidad de Lodz
Peter Rowland, Packet Clearing House
Michael Schmitt, Facultad de derecho de Exeter

Patra Kongsirimongkolchai / EyeEm / Getty Images

SECRETARIADO

The Hague Centre for Strategic Studies

EastWest INSTITUTE

ASOCIADOS

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

PATROCINADORES

Departamento Federal de Asuntos Exteriores de Suiza

GLOBSEC

Ministerio de Asuntos Exteriores de Estonia

Ministerio de Asuntos Internos y Comunicaciones de Japón

COLABORADORES

Comisión de la Unión Africana

Black Hat USA

DEF CON

Delegación de la Unión Europea ante las Naciones Unidas en Ginebra

Foro Global de Especialistas en Ciberseguridad

Google

Municipio de La Haya

Packet Clearing House

Universidad de Tel Aviv

Instituto de las Naciones Unidas de Investigación sobre el Desarme