Tema central

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2576

URVIO, Revista Latinoamericana de Estudios de Seguridad. No. 20, Quito, junio 2017, pp. 16-30
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea)

La política brasileña de ciberseguridad como estrategia de liderazgo regional

The brazilian cybersecurity policy as a strategy of regional leadership

Luisa Cruz Lobato[1]

Fecha de recepción: 13 de febrero de 2017
Fecha de aceptación: 26 de abril de 2017

Resumen

El artículo analiza la estructuración de la política de ciberseguridad de Brasil entre los años de 2003 y 2016 como componente de su estrategia de inserción internacional y proyección de liderazgo en el Sul Global. El campo de la gobernanza de la Internet, de lo cual la ciberseguridad es parte, ofrece al país una oportunidad de relativo bajo costo de protagonismo en la elaboración de normas internacionales. Analizase documentos principales de esa política y argumentase que ella es parte de los esfuerzos de proyección del *soft power* del país en el campo de la seguridad internacional, pero que sus incoherencias pueden afectar y hasta mismo comprometer esta estrategia. Por fin, trazase breves proyecciones para esta política ante los cambios políticos en Brasil.

Palabras clave: Brasil; ciberseguridad; gobernanza de internet; liderazgo regional.

Abstract

The article analyzes the structuration of Brazil's cybersecurity policy between the years of 2003 and 2016 as a component of its strategy of international insertion and projection of leadership in the Global South. The Internet governance field, of which cybersecurity is a part, offers the country a relatively low-cost opportunity of protagonism in the elaboration of international norms. It analyzes cornerstone documents of this policy and argues that it is a part of the country's efforts to project its *soft power* in the field of international security, but that its incoherencies can affect and even compromise the strategy. Finally, it draws brief projections to this policy in face of political changes in Brazil.

Keywords: Brazil; cybersecurity; internet governance; regional leadership.

1Estudiante del Doctorado en Relaciones Internacionales de la Pontificia Universidad Católica de Rio de Janeiro (PUC-Rio) y Máster en Relaciones Internacionales con mención en Política Internacional por la misma institución. Investigadora visitante del grupo de práctica jurídica en Derechos Humanos del Centro Universitário do Pará (CESUPA). Correo: l.cruzlobato@gmail.com

Introducción

La "revolución digital" en Latinoamérica ha sido poco homogénea y significativamente desigual. Los principales desafíos comunes para la región incluyen la mejora de las condiciones de acceso a la red –apenas la mitad de la población está conectada a internet – y la poca atención dada a la ciberseguridad. Según el Banco Interamericano de Desarrollo, cuatro de cada cinco países latinoamericanos carecen de una estrategia de ciberseguridad (BID 2016). A diferencia de la mayor parte del subcontinente, en las últimas décadas se presenció el esfuerzo de Brasil para estructurar una política propia de ciberseguridad motivada en parte por las amenazas percibidas tras el exponencial crecimiento de usuarios de internet en el país y en parte por su envolvimiento activo con la agenda internacional de gobernanza de Internet.

La agenda de ciberseguridad se muestra bastante atractiva a los intereses estratégicos del país (Diniz, Muggah y Glenny 2014). Sin embargo, la política brasileña enfrenta significativos desafíos, tales como el problema de la especificación de las amenazas y la implementación y administración de esta política en la práctica. El objetivo de este artículo es analizar la arquitectura institucional y los principales instrumentos normativos de la política brasileña de seguridad cibernética para comprender su inserción en la estrategia de proyección internacional del país. Se argumenta, que por vía de la exportación de sus experiencias internas con ciberseguridad, Brasil ha intentado proyectar regional e internacionalmente su "soft power" en la agenda de la gobernanza de internet, pero las incoherencias en su política doméstica pueden afectar y hasta comprometer la estrategia.

El artículo se divide en cuatro partes. En la primera, se abordan los temas de gobernanza de internet y ciberseguridad en las relaciones internacionales, discutiéndose la relación entre ambas y argumentándose que la ciberseguridad es un componente fundamental de la gobernanza de Internet, pero posee lógicas de gestión propias (DeNardis y Raymond 2013). En la segunda parte, se analiza la arquitectura institucional y los principales instrumentos normativos que componen la política de ciberseguridad brasileña, señalando sus características y principales problemas. La metodología utilizada comprende un relevamiento de los principales instrumentos normativos y legales que estructuran la política, destacándose la "Estratégia Nacional de Defesa", la "Política Cibernética de Defesa" y la "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Adm*i*nistração Pública Federal (2015-2018)".

En la tercera parte, se analiza el lugar de la ciberseguridad en la estrategia de inserción internacional de Brasil, argumentándose que la política desarrollada internamente es vista como instrumento de proyección de su *soft power*, mediante la exportación de prácticas exitosas, lo que es auxiliado por la actuación del país en procesos de elaboración de normas/prácticas internacionales relativas a la gobernanza de Internet, así como por la respuesta de la estructura existente. En la cuarta y última parte, se traza una breve perspectiva para la ciberseguridad en Brasil tras los cambios políticos recientes en el país.

Gobernanza de Internet y ciberseguridad

En los últimos años, el creciente reconocimiento de la Internet, como una infraestructura básica de soporte económico y social de

las vidas, ha llamado la atención sobre cuestiones relativas a su gobernanza, lo que incluye las funciones, instituciones y sistemas técnicos necesarios para mantenerla operacional y segura (DeNardis y Musiani 2016). Lo que se comprende por gobernanza de Internet abarca desde las cuestiones de infraestructura, coordinación técnica y política relativas al intercambio de información por medio de la red, hasta las disputas y deliberaciones acerca de la manera como ella es coordenada, administrada y modelada para reflejar políticas (DeNardis 2009; Mueller 2010).

Tradicionalmente, el foco de la mayor parte de los estudios sobre el tema han sido el conjunto de instituciones e instrumentos políticos que comprenden la coordinación global del Dominio de Nombres y Números (DNS) y otras atribuciones de normas de configuración (van Eeten y Mueller 2012). Diversas investigaciones han prestado atención a las controversias sobre las tareas realizadas por la Corporación para Nombres y Números Asignados (ICANN), procesos en las Naciones Unidas, a ejemplo de la Cumbre Mundial sobre la Sociedad de la Información (WSIS) y del Fórum para la Gobernanza de Internet (IGF), y en disputas sobre el modelo (multisectorial o multilateral) más adecuado a toma de decisiones políticas para la Internet (Dutton 2015; DeNardis y Raymond 2013; Maciel y Souza 2011). Conceptualmente, la atención de la literatura a las instituciones, al Estado y a la regulación apunta hacia la fuerte influencia de investigaciones jurídicas y de relaciones internacionales en esos dichos estudios (Epstein, Katzenbach y Musiani 2016; Flyverbom 2016).

Definiciones como la de Mueller (2010), para quien la gobernanza de Internet se ha vuelto una plataforma para disputas sobre una gama de políticas informacionales y de comunicación, aclaran la manera de cómo las relaciones internacionales influencian la literatura de la gobernanza de Internet. El autor justifica el uso del término "gobernanza" en razón de su "debilidad" en relación con el concepto de gobierno y lo equipara a su uso en las relaciones internacionales:

> El término gobernanza, sin embargo, ganó circulación en las relaciones internacionales precisamente porque era más débil que gobierno; denota la coordinación y regulación de actores interdependientes en ausencia de una autoridad política global. En las relaciones internacionales, el término gobernanza global sugiere que existe alguna función de dirección y organización, pero que es menos jerárquica y autoritaria (Mueller 2010, 8-9).

Sin embargo, el término "gobernanza de Internet" puede ser engañoso al sugerir la idea de un proceso único (Dutton 2015). La especificidad de cada función de la gobernanza de la Internet, resulta en una forma propia de coordinación y en la participación de actores distintos en ella. Como argumentan DeNardis y Raymond (2013), el proceso de gobernanza de Internet comprende varias clases de tareas diferentes y lo que la mantiene operacional es una costosa coordinación administrativa entre los actores primarios envueltos en estas tareas. En la práctica, esto significa comprender que el control de los "recursos críticos" de la Internet, por ejemplo, el servicio de DNS, no opera de la misma manera que la gobernanza de la ciberseguridad o que la definición de los estandartes de la Internet. En el caso de la ciberseguridad, su operación incluye desde las actividades las compañías de *software* responsables por la corrección de vulnerabilidades en

sus productos hasta la operación de respuestas a problemas de seguridad, lo que incluye las actividades de los Centros de Estudio de Respuestas y Tratamiento de Incidentes (CERTS).

Es posible decir que la ciberseguridad es una de las funciones comprendidas por la agenda de la gobernanza de Internet (Mueller 2010; DeNardis y Raymond 2013; Oppermann 2014). No se limita a la protección y reacción contra amenazas perpetradas por medio del ciberespacio, lo que incluye el uso de una serie de medidas utilizadas para evitar que un sistema sea comprometido por terceros. También responde a problemas de seguridad en Internet, como ataques de denegación de servicio, asegura la protección de datos de la identidad y el correcto funcionamiento de los sistemas digitales (Nissenbaum 2005; Deibert y Rohozinsk 2010). De una perspectiva más técnica, la ciberseguridad aún abarca el desafío de asegurar las infraestructuras necesarias al funcionamiento de la Internet, lo que incluye, además de ofrecer respuestas a problemas de seguridad en Internet, el enrutamiento, la autenticación de sistemas y el DNS (DeNardis y Raymond 2013).

En las últimas décadas, el tema recibió vasta atención en la literatura de las relaciones internacionales (Barnard-Wills y Ashenden 2012; Dunn Cavelty 2008; 2012; 2015; 2016; Deibert 2011; 2013; Deibert y Rohozinski 2010; Eriksson y Giacomello 2009; Hansen y Nissenbaum 2009; Nissenbaum 2005). Una cartografía hecha por Dunn Cavelty (2016), sugiere que la mayor parte de la producción académica en la disciplina puede ser dividida en los siguientes grupos: un grupo de trabajos producidos por expertos enfocados a discutir la formulación de políticas, generalmente en el ámbito de los "think-tanks" (CSIS 2008; 2010; Ablon, Libicki y Golay 2014), estudios críticos enfocados en la relación entre información y poder (Day 2001), estudios sobre la producción de inseguridad en la Internet a partir de prácticas de vigilancia y censura (Deibert *et al.* 2010) y estudios sobre la constitución de amenazas en el ciberespacio (Dunn Cavelty 2008; Hansen y Nissenbaum 2009; Betz y Stevens 2013).

En determinados países, la recurrente asociación entre riesgos y vulnerabilidades digitales y la seguridad nacional, así como el constante énfasis en la posibilidad de ciberataques catastróficos, los cuales son simbolizados por escenarios donde las infraestructuras críticas de un país son comprometidas por ellos, han puesto las amenazas a la ciberseguridad en una condición de peligros calamitosos, inminentes y urgentes, llevando a un proceso de securitización de esas amenazas. Esa interpretación de las amenazas cibernéticas ha generado críticas por ser considerada extremamente improbable (Rid 2012), así como considerables preocupaciones con el recurso a la militarización del ciberespacio como respuesta a ellas (Dunn Cavelty 2012). Recientemente, se ha dado renovada atención al lazo entre gobernanza de Internet y la ciberseguridad, desde que los problemas de ciberseguridad han desafiado cada vez más las instituciones existentes de gobernanza de Internet, a ejemplo de los conflictos de jurisdicción y tentativas de control de diferentes Estados sobre los servicios de Internet (Mueller, Schmidt y Kuerbis 2013; Mueller y Klein 2014; Internet Governance Project 2016).

Es relevante establecer la asociación entre ciberseguridad y gobernanza de la Internet, pues ella proporciona un punto de partida para el análisis del desarrollo de la política de ciberseguridad en Brasil, así como resaltar sus características y principales problemas. Esto

porque comprender la ciberseguridad como una función de la gobernanza de Internet permite entender la participación de Brasil en esas agendas a partir de una estrategia amplia de inserción internacional puesta en práctica por el gobierno brasileño entre los años 2003 y 2015 y que ha priorizado las relaciones Sur-Sur y la proyección política de Brasil como un liderazgo regional y del "Sur Global". Esa estrategia y sus limitaciones, a su vez, pueden ser mejor explicadas y comprendidas tras un análisis cuidadoso de los principales puntos y características de la política brasileña de ciberseguridad.

La política de ciberseguridad de Brasil

La política de ciberseguridad brasileña se ha desarrollado en un contexto de creciente preocupación con el incremento en el número de ataques cibernéticos y por la capacidad del país de hacer frente a ellos, así como por la oportunidad de no quedar detrás de las principales potencias mundiales en el enfrentamiento de las amenazas cibernéticas (Abdenur 2014). Brasil está en la lista de los países más *atingidos* (golpeados) por el cibercrimen tanto por origen de actividades criminales, como por el número de víctimas de esas actividades (Muggah y Thompson 2015). En 2013, diversos sitios del gobierno federal fueron blancos de ataques cibernéticos y en el mismo año, el país se descubrió afectado por las actividades de espionaje en masa de los EEUU. Esos eventos fueron acompañados de un creciente número de individuos en el país con acceso a la Internet: hoy, cerca de 67.5% de su población se encuentra conectada (Internet World Stats 2016).

En función de ese escenario y del intenso envolvimiento de Brasil con las agendas internacionales de ciberseguridad y gobernanza de Internet, se vuelve importante comprender el proceso de desarrollo y las características de su política de ciberseguridad, así como señalar sus posibles incongruencias. Para este fin, el análisis se centra principalmente en tres documentos: la "Estratégia Nacional de Defesa" (END), la "Política Cibernética de Defesa" (PCD) y la "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015-2018)" (Estrategia de Ciberseguridad) y se utilizan también estudios sobre la estrategia de seguridad de Brasil para el ciberespacio como bibliografía secundaria.

Arquitectura institucional

Los esfuerzos de defensa y seguridad cibernéticas en Brasil suceden en un contexto de iniciativas de reestructuración interna y fortalecimiento de la capacidad de defensa nacional iniciada en 1999 con la creación del Ministerio de la Defensa (Abdenur 2014). La estructura de la ciberseguridad hoy es descentralizada, o sea, no hay un liderazgo central que coordine el tema en el gobierno, y orbita en torno de la distinción a nivel conceptual e institucional entre seguridad y defensa cibernéticas: la primera comprende la prevención y represión, mientras la segunda se refiere a las acciones operacionales de combates ofensivos (Mandarino Junior y Canongia 2010; Cruz Júnior 2013).

En el ámbito del Gobierno Federal se establece un sistema jerárquico para la toma de decisión estratégica desde la Presidencia de la República hasta el nivel operacional, cuyas acciones en materia de seguridad cibernética son coordinadas por el "Gabinete de Segu-

rança Institutional da Presidência da República" (GSI-PR), mientras la coordinación de la defensa queda a cargo del "Centro de Defesa Cibernética" (CDCiber), vinculado al Ejército brasileño y al Ministerio de la Defensa. A pesar de que ambos están jerárquicamente abajo de la Presidencia de la República, no existe una agencia propia responsable por la implementación de su estrategia y política de ciberseguridad, estando la competencia un tanto dividida entre órganos como el Consejo Nacional de Defensa, que coordina la política y estrategia de defensa nacional, el GSI-PR, el Ejército, mediante el CDCiber, la Agencia Brasileña de Inteligencia (ABIN) y el Ministerio de la Justicia, por medio de la Policía Federal.

El GSI-PR, extinto en 2015 y restablecido por fuerza de la ley 13.341 de 29 de septiembre de 2016, es responsable por prestar asistencia a la Presidencia de la República en asuntos militares y de seguridad, así como coordinar las actividades de inteligencia federal y seguridad de la información. El Departamento de Seguridad de Información y Comunicación (DSIC-GSI), órgano que compone el gabinete, es directamente responsable por la coordinación de acciones de seguridad cibernética, lo que incluye la operación y manutención de un centro de tratamiento de incidentes en las redes de la Administración Pública Federal (APF).

La Estrategia de Ciberseguridad estableció metas de mejoramiento de la seguridad y resiliencia de las infraestructuras críticas y servicios públicos nacionales para el período de 2015 a 2018. Entre los principales objetivos de la Estrategia, se encuentran el aumento del volumen de recursos presupuestarios de la ciberseguridad y una articulación y coordinación más orientadas para el tema en el ámbito de la administración pública. El CDCiber, creado en 2010, volviéndose operacional entre los años de 2011 y 2012. El centro se encuentra entre los niveles estratégico y operacional del gobierno, a vez que es subordinado al Ministerio de la Defensa, lo cual lo somete al GSI-PR. La estrategia del CDCiber incluye actividades cibernéticas en las áreas de la inteligencia, ciencia y tecnología, habilidades operacionales, doctrina y recursos humanos; su misión consiste en la protección de las redes militares y gubernamentales de ciberataques. Entre las actividades y proyectos del centro, están, por ejemplo, la administración de la seguridad de informaciones durante los megaeventos que tuvieran lugar en Brasil entre los años de 2014 y 2016 (Portal Brasil 2015).

La piedra angular de la política de defensa brasileña es la END, presentada por el Ministerio de la Defensa, aprobada por el Decreto nº 6.703 de 18 de diciembre de 2008, y revisada en 2012. El objetivo de la estrategia es elaborar un plan de defensa a medio y largo plazo y, así, modernizar la estructura nacional de defensa. La END ha establecido el ciberespacio, junto a los sectores aeroespacial y nuclear, como estratégico para el desarrollo y autonomía nacionales y ha delegado el liderazgo de la defensa cibernética al Ejército (la Armada y la Fuerza Aérea son encargadas de los programas nuclear y aeroespacial, respectivamente). La versión revisada del documento establece como prioridad el fortalecimiento del CDCiber para que este se convierta en el Comando de Defensa Cibernética de las Fuerzas Armadas. Además del CDCiber, del GSI-PR y de los otros órganos ya mencionados, agregan la política de protección cibernética brasileña: el Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad (CERT), del Servicio Federal de Procesamien-

to de Dados (Serpro), de centros de investigación en asociación con el gobierno y otros órganos responsables por la administración de sistemas.

La "securitización" de la ciberseguridad

La noción de "securitización" en la teoría de las relaciones internacionales dice respecto al movimiento de inserción de un determinado asunto en la agenda de seguridad a partir de su construcción como amenaza existencial o condición de emergencia frente al Estado (Buzan, Waever y Wilde 1998). Una vasta literatura ha discutido el proceso de securitización de la ciberseguridad de manera general (Dunn Cavelty y Jaeger 2015; Hansen y Nissenbaum 2009; Dunn Cavelty 2008; Bendrath, Eriksson y Giacomello 2007; Nissenbaum 2005) y de manera más específica en el caso brasileño (Lopes 2013; Diniz, Muggah y Glenny 2014). Aquí se utiliza el término para hacer referencia a un esfuerzo en curso que comprende desde la politización[2] de un tema hasta su eficaz inserción, o no, en la agenda de seguridad.

El desarrollo de la política de ciberseguridad en Brasil coincide con una serie de percepciones de las amenazas cibernéticas como una cuestión existencial de seguridad (Mandarino Junior y Canongia 2010). El documento oficial más importante en ese sentido, es la END, ya que incluye el asunto entre aquellos estratégicos para el desarrollo y defensa del país (Brasil 2008). La estrategia contextualiza esa necesidad en razón de las vulnerabilidades traídas por los avances tecnológicos de la información, y su adopción por diversos países en el mundo. Ilustran dicho escenario, la proyección de la ciberseguridad en foros internacionales sobre sociedad de la información y gobernanza de Internet, el aumento del número de ataques a redes gubernamentales, así como eventos de amplia repercusión como los ataques cibernéticos contra Georgia (2007) y Estonia (2008), y más tarde, el descubrimiento del *worm* Stuxnet que afectó las operaciones de instalaciones nucleares en Irán (2010).

Los principios de la política de ciberseguridad brasileña están en el Decreto nº 3.505/2000 que instituyó la política de seguridad de la información en entidades y organismos de la APF. El decreto atribuye como presupuestos básicos de la APF la capacitación tecnológica del país para uso de la criptografía en la seguridad y defensa del Estado, así como el fortalecimiento de la seguridad de información. Desde entonces, diversos mecanismos normativos han sido publicados con vista a la regulación de la seguridad de información en el ámbito de la APF hasta la inclusión del sector cibernético en la END y su atribución al Ejército.

El Ministerio de la Defensa aprobó en 2012 la Política Cibernética de Defensa (Portaria Normativa nº3.389/MD de 21 de Dezembro de 2012), que establece los principios, objetivos y directrices para las actividades en ese sector. El hecho de que dos de los tres principales documentos analizados están en el ámbito del Ministerio de la Defensa (y, por consecuencia, del Ejército) ha levantado críticas a un proceso visto como excesivamente militarizado. Uno de los principales argumentos en ese sentido

2 La relación entre securitización y politización comprende un *continuum* que abarca desde la ausencia de un asunto en las políticas estatales y debates públicos, hasta su inserción en estas agendas, cuando entonces el asunto se vuelve objeto de políticas públicas, y posible securitización, cuando el asunto entonces se vuelve amenaza a la existencia del Estado, demandando medidas de emergencia o la toma de decisiones fuera de las reglas ordinarias de los procedimientos políticos. Ver Buzan, Waever y Wilde (1998).

es la existencia de un desequilibrio en la balanza de amenazas y respuestas, lo que resulta en el manejo inapropiado de las amenazas cibernéticas, con un enfoque mayor en aquellas poco probables, como la guerra cibernética, en detrimento de una mejor preparación para enfrentar cuestiones más urgentes, como el cibercrimen (Diniz, Muggah y Glenny 2014).

La división entre seguridad y defensa cibernética desde los principios del tratamiento de Brasil sobre el tema también ha sido criticada. Se argumenta que la separación tiende a fragilizar la seguridad cibernética, pues esta pasa a depender de la afinidad y coordinación de los dirigentes del CDCiber/Ministerio de la Defensa y del GSI-PR, además de favorecer ambas sobre posición de tareas y brechas por indefinición de responsabilidades (Cruz Júnior 2013), lo que hace bastante confusa la arquitectura institucional de la ciberseguridad en el país. Mas aún, la separación institucional entre ciberseguridad (civil) y defensa (militar) no impidió la actuación del CDCiber en los Juegos Olímpicos y Paralímpicos en el país (Portal Brasil 2015).

Fuera del ámbito de la defensa, la Estrategia de Ciberseguridad del GSI-PR establece las principales metas y objetivos estratégicos para las áreas de seguridad de la información y ciberseguridad. Ella fue antecedida por el "Livro Verde sobre Segurança Cibernética no Brasil", que estableció las directrices estratégicas para una política de seguridad cibernética en el corto, medio y largo plazos. La estrategia contiene diez objetivos y se propone, en conformidad con los vectores propuestos en el documento que la procedió, la promoción de Brasil como actor protagonista en la ciberseguridad a partir de inversiones internos en tecnologías de información, la creación de empleos, el establecimiento de asociaciones con el sector privado, la reducción de la dependencia de tecnologías externas, mejorar la gestión de la ciberseguridad en el ámbito de la APF; así como promover la concienciación de la población acerca de la seguridad cibernética, entre otros.

La Estrategia de Ciberseguridad, al igual que los documentos orientados a la defensa ha traído una respuesta, aunque parcial, a la cuestión de que Brasil tenga o no una política de ciberseguridad. Esta respuesta no está libre de críticas, las cuales incluyen su imprecisión y poca consideración de principios de derechos humanos en su aplicación (Artigo 19 2016). Además, los objetivos de la estrategia no hacen referencia directa a su contraparte de defensa, señalando una intención de mantener la separación entre defensa y seguridad cibernética en el conjunto de la política de ciberseguridad brasileña. Por otra parte, tanto la estrategia cuanto su documento predecesor, llaman la atención para el deseo de Brasil, por medio de sus políticas de ciberseguridad, de volverse un jugador internacional en el área (Mandarino Junior y Canongia 2010; Brasil 2015).

Brasil, la ciberseguridad y las relaciones internacionales

En las últimas décadas se ha visto un esfuerzo por parte de Brasil para consolidarse como un jugador relevante en diferentes aspectos de la gobernanza global. El país es parte de un grupo que, en el mismo período, experimentó un crecimiento económico significativo y adquirió influencia política a un nivel internacional (Zakaria 2008; Alden, Morphet y Vieira 2010; Stuenkel 2015). Abrazando el concepto de "Sur Global", Brasil y otros países que pasaban por un proceso similar intentaron pro-

yectar como liderazgos en diferentes negociaciones multilaterales (Stuenkel 2015).

La relevancia de la ciberseguridad para la agenda política brasileña debe ser pensada a partir de su participación en procesos de toma de decisiones y elaboración de normas sobre la gobernanza de la Internet. Brasil ha acompañado el desarrollo del debate desde su principio, abogando por cambios en la arquitectura de la gobernanza de la Internet (Maciel, Zingales y Fink 2015). En la esfera internacional, la intensificación de los debates sobre el asunto acompañó el establecimiento del IGF tras el segundo encuentro de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en 2005 (WSIS 2005).

Brasil ha participado activamente de todas las ediciones del IGF, habiendo sido su anfitrión en 2003, cuando tuvo lugar en Río de Janeiro y, en 2014, en João Pessoa. En ese proceso, ha defendido el fortalecimiento de un modelo multisectorial de gestión para la Internet (Opperman 2014; Maciel, Zingales y Fink 2015). El modelo multisectorial, comprende el reconocimiento del papel de actores de naturalezas distintas en la estructuración y gestión de la Internet y propone que las discusiones y debates ocurran en un nivel horizontal, en vez de jerárquico. La importancia de ese modelo se asocia al propio desarrollo histórico de la Internet, que al principio funcionaba como una red de comunicación académica entre institutos de investigación en los EEUU en los años de 1960, y más tarde, en los años 1990, vio la participación de actores comerciales y gobiernos aumentar exponencialmente (Castells 2010).

Para defender la agenda, Brasil ha utilizado su propia experiencia con debates multisectoriales en asuntos relacionados a la Internet. El Comité Gestor de la Internet (CGI.br), creado en 1995, es responsable por establecer las directrices para el uso y desarrollo de la Internet en el país, lo que incluye la asignación de dirección "IP" (Internet Protocol) y la administración del dominio de primer nivel ".br"[3], entre otras decisiones administrativas y operacionales. El CGI.br es un órgano de carácter multisectorial en su composición y proceso de deliberación, compuesto por 21 miembros: nueve representantes del gobierno, cuatro del sector empresarial, cuatro de la sociedad civil, tres de la comunidad científica y tecnológica, y un representante de notorio saber en asuntos de la Internet.

Ese compromiso con la agenda de gobernanza de la Internet, fue luego complementado por el crecimiento de la importancia de la ciberseguridad (considerada uno de los tópicos centrales de la gobernanza de Internet por el IGF) para la agenda política del país, y fue motivada por el aumento en el número de personas conectadas a la Internet, acompañado por el aumento en el número de ciberataques contra individuos y entes públicos, y por la proyección global de ese tipo de evento, a ejemplo de lo ocurrido en Georgia, Estonia e Irán. La ciberseguridad puede ser pensada como parte de una tendencia más amplia de expansión del significado de la seguridad internacional en las décadas posteriores a la Guerra Fría, quedándose frecuentemente en la categoría de amenazas no tradicionales (Abdenur 2014). Sin embargo, en las relaciones internacionales no hay consenso acerca de su definición o potencial transformativo, a vista de las discordancias sobre la dimensión de la real amenaza puesta por las amenazas cibernéticas (Abdenur 2014; Rid 2012). Además,

3 Para una relación de todas las atribuciones del CGI.br, ver el Decreto nº 4.829, de 3 de septiembre de 2003.

el reconocimiento del ciberespacio como sitio de conflicto entre naciones y su creciente importancia en las agendas de seguridad de los países (NATO, 2016), señalan la importancia de desarrollar recursos propios para su análisis y tratamiento.

Para Brasil, las tecnologías de la información pasaron a representar una oportunidad de redistribución de recursos para el desarrollo, posibilitando la reversión de la tendencia de concentración de renta por los países desarrollados (Fontenelle 2012; Cruz Júnior 2013; Keohane y Nye 1998). Las políticas de inclusión digital en el país resultaron en un aumento exponencial en el número de personas conectadas a la Internet, lo que no fue acompañado de una concientización de los usuarios sobre los riesgos digitales. Así, el empoderamiento digital ha moldado el ciberespacio brasileño, confiriéndole amplia escala y dinamismo, que incluye la dimensión que el cibercrimen adquirió en el país (Diniz, Muggah y Glenny 2014; Muggah y Thompson 2015).

La gobernanza global de la ciberseguridad es un proceso aún en curso y precisamente por eso, pone oportunidades y desafíos de defensa y política externa para potencias en ascensión que buscan mayor influencia global. La escasez de recursos para inversión, si comparada a la de las principales potencias mundiales y la competición interna con otras agendas políticas y de seguridad, son apuntados como dos de los principales problemas enfrentados en la consolidación de una agenda coherente para la ciberseguridad en Brasil, como en otras potencias en ascenso (Cruz Júnior 2013; Abdenur 2014). Además, se acredita que, por estar en una fase de desarrollo inicial también en el resto del mundo, el momento presenta una oportunidad para que el país se proyecte internacionalmente (Mandarino Junior y Canongia 2010; Cruz Júnior 2013). Si se comparan con los esfuerzos brasileños con otras áreas de la política internacional, como los gastos militares y las operaciones de paz, ambas la gobernanza de Internet y de ciberseguridad aún son percibidas como agendas menos costosas (Diniz, Muggah y Glenny 2014).

Abdenur (2014) nota que hace poco tiempo que las relaciones internacionales comenzaron a tratar de las cuestiones de poder producidas por la ciberseguridad. Sin embargo, la relación entre poder y tecnologías de la información, más ampliamente consideradas, es discutida por Keohane y Nye (1998). Los autores argumentan que esas tecnologías alteran patrones de interdependencia compleja al aumentar la cantidad de canales de comunicación en la política mundial y tienden a volverse importantes recursos de poder en la política mundial. Nye (2004) sostiene que la era de la información aumenta la relevancia del "*soft power*" y que este tenderá a tornarse menos una función de recursos materiales.

La estrategia de proyección del *soft power* es adoptada por Brasil en la agenda de gobernanza de Internet, particularmente considerándose sus esfuerzos para influenciar la elaboración de normas internacionales sobre asuntos que abarcan desde el cibercrimen, con su crítica abierta a la Convención de Budapest e iniciativa para discutir una convención global sobre el tema (Diniz, Muggah y Glenny 2014), hasta su defensa del modelo multisectorial en el IGF. Las revelaciones de Edward Snowden en 2013 acerca de la estrategia de espionaje global de los Estados Unidos, llevaran no solo a una intensificación de los esfuerzos del país para influenciar la elaboración de normas sobre o tema, a ejemplo de la iniciativa conjunta con Alemania de una resolución

sobre privacidad online ante la Organización de las Naciones Unidas, que ha resultado en la designación de un Relator Especial sobre el Derecho a Privacidad, como también en una mayor atención de Brasil para sus vecinos de América del Sur y en los BRICS (Brasil, Rusia, India, China, Sudáfrica). [4]

Regionalmente, se apunta para acuerdos de cooperación en el marco de la Unión de Naciones Suramericanas (UNASUR) y del Consejo de Defensa Suramericano (CDS), entre Brasil, Argentina y Chile (Justibró 2014). En esos acuerdos están incluidos esfuerzos para fortalecer la colaboración en el área cibernética, lo que comprende ampliar la capacitación en seguridad de información y criptografía, métodos y sistemas tecnológicos, así como el intercambio de integrantes de Equipos de Respuestas de Incidentes de Seguridad Informática (CSIRTs, en inglés) y de investigación científica.

Además de los acuerdos bilaterales, Brasil busca aún exportar para sus vecinos el aprendizaje con la actuación del CDCiber en la seguridad de los Juegos Olímpicos de Rio de Janeiro y de la Copa del Mundo de Fútbol. Por otra parte, el establecimiento de la Escuela de Defensa Suramericana (ESUDE) ha sido visto como una oportunidad para la ampliación de la colaboración con defensa cibernética en la región (Abdenur 2014; Ministério da Defesa 2016b). Sin embargo, para que las iniciativas de cooperación e integración regional en Latinoamérica sean exitosas, es relevante que Brasil busque acercarse a sus vecinos, en particular de los países miembros de UNASUR, a fin de construir una visión compartida acerca de las fuentes comunes de seguridad e inseguridad en Sudamérica y de superar los obstáculos a la cooperación para la ciberseguridad en la región (Justribó 2014).

Consideraciones finales

La intensa participación de Brasil en asuntos relacionados a la gobernanza de la Internet le ha otorgado una posición de actor protagonista en el campo. Una de las vías adoptadas por el país ha sido la proyección de políticas relacionadas a la Internet como una estrategia de *soft power*, entre las cuales se encuentra la ciberseguridad (Diniz, Muggah y Glenny 2014). Pero la posición brasileña con relación al asunto, es también influenciada por su condición de potencia en ascensión y por las contradicciones que de eso transcurren: hay una tentativa por parte del país de equilibrar sus aspiraciones de jugar un papel más amplio en la política internacional (particularmente en la seguridad), al mismo tiempo en que hay limitaciones significativas a su capacidad de actuar en el exterior (Abdenur 2014).

La estrategia brasileña para la ciberseguridad y gobernanza de Internet, tiene significativas contradicciones que resultan en gran parte de problemas institucionales y administrativos de sus políticas y de la adopción de prioridades equivocadas. Una división institucional como la establecida en la política brasileña y la falta de principios claros en la estrategia puede llevar a posiciones y actitudes contradictorias, como bien señala el caso de la vigilancia de la ABIN y del CDCiber sobre la población brasileña en ocasión de las protestas de 2013, en total contrapunto a las duras críticas hechas por la presidente brasileña al espionaje estadounidense. Las incohe-

4 Sin embargo, en el caso de los BRICS, la cooperación parece más costosa: paralizada desde 2015, la construcción de un cabo submarino alternativo fuera del occidente está siendo continuada por la China (Lee (2017).

rencias entre la política interna y la posición internacional de Brasil, pueden generar tres efectos: afectar significativamente la posición que el país viene intentando intenta construir internacionalmente para sí en la agenda de gobernanza de Internet, debilitar los esfuerzos existentes de integración y cooperación regional en Latinoamérica, y dejar su política de ciberseguridad más susceptible a cambios políticos internos y externos.

Tras los cambios políticos que resultaron de la destitución de la presidente Dilma Rousseff, hubo esfuerzos para reestructurar el sector de inteligencia bajo la coordinación del nuevo GSI-PR. La Estrategia de Ciberseguridad esta mantenida bajo la nueva coordinación del órgano, mientras que la política de defensa debe pasar por un proceso de revisión periódica en lo cual, al que todo indica, la ciberseguridad debe mantener su importancia estratégica (Ministério da Defesa 2016a). Asimismo, en noviembre de 2016, el GSI-PR y el Ministerio de la Defensa anunciaran estar en vías de construir una estrategia conjunta de cooperación interministerial para la seguridad y defensa, en la cual la agenda cibernética es considerada una de las prioridades. No hay indicativos de cambios sustantivos en la arquitectura institucional de la ciberseguridad en el gobierno al corto y mediano plazos y la tendencia es su manutención, con todos los problemas de atribución que la acompañan.

Es deseable que Brasil desarrolle una política de ciberseguridad más coherente con los problemas de seguridad que enfrenta y que esté más atenta al escenario regional, y que se coopere con el sector privado para reducir los costos del cibercrimen no solo para las empresas, también para el usuario de Internet. Superar la fragmentación en su arquitectura institucional es fundamental para que las iniciativas de ciberseguridad en el país y en cooperación con sus vecinos sean más coherentes. Investigaciones futuras en el área de ciberseguridad, deben considerar no apenas esfuerzos en ese sentido, como también las iniciativas de cooperación regional e internacional del país en materia de ciberseguridad, así como la participación del sector privado tanto en la estrategia nacional cuanto en la construcción de un papel global más protagonista para el país.

Bibliografía

Abdenur, Adriana. 2014. "Brazil and Cybersecurity in the Aftermath of the Snowden Revelations". En *International Security: a European-South American Dialogue*, 229-283. Río de Janeiro: Konrad-Adenauer-Stiftung.

Ablon, Lillian, Martin C. Libicki y Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Mónica: RAND.

Alden, Chris, Sally Morphet y Marcos Antonio Vieira. 2010. *The South in World Politics.* Basingstoke: Palgrave Macmillan.

Artigo 19. 2016. *Brasil: Análise da Estratégia de Cibersegurança.* São Paulo: Artigo.

Balzacq, Thierry. 2011. "A theory of securitization: origins, core assumptions, and variants". En *Securitization theory: how security problems emerge and dissolve*. Nueva York: Routledge.

Barnard-Wills, David, y Debi Ashenden. 2012. "Securing Virtual Space: Cyber War, Cyber Terror and Risk". *Space and Culture*: 110-123.

Bendrath, Ralf, Johan Eriksson, e Giampero Giacomello. 2007. "From 'cyberterror-

ism' to 'cyberwar', back and forth: How the United States securitized cyberspace". *International Relations and Security in the Digital Age*, J. Eriksson y G. Giacomello, 57-82. Nueva York: Routledge.

Betz, David J., y Tim Stevens. 2013. "Analogical reasoning and cyber security". *Security Dialogue*: 147-164.

BID (Banco Interamericano de Desarrollo). 2016. "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?", https://publications.iadb.org/handle/11319/7449?locale-attribute=es&.

Brasil. 2015. *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018.* Brasilia: Presidência da República.

_____. 2012. *Política Cibernética de Defesa.* Brasilia: Ministério da Defesa.

_____. 2008. *Estratégia Nacional de Defesa.* Brasilia: Ministério da Defesa.

Buzan, Barry, Ole Waever, y Jaap de Wilde. 1998. *Security: a New Framework for Analysis.* Londres: Lynne Rienner Publishers.

Castells, Manuel. 2010. *The rise of the network society.* Malden: Blackwell.

Cruz Júnior, Samuel Souza da. 2013. *A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual.* Río de Janeiro: IPEA.

CSIS. 2010. *Cybersecurity two years later: a report of the CSIS Commission on Cybersecurity for the 44th Presidency.* Washington DC: Center for Strategic and International Studies.

CSIS. 2008. "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency". Center for Strategic and International Studies, Washington DC, 90.

Day, Ronald E. 2001. *The Modern Invention of Information: Discourse, History and Power.* Carbondale: Southern Illinois University Press.

Decreto nº4.829/2003, de 3 de setembro, dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil e dá outras providências (D.O.U de 4 de setembro de 2003).

Decreto nº3.505/2000, de 13 de junho, institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal (D.O.U de 14 de junho de 2000).

Deibert, Ronald J. 2013. *Black Code: inside the battle for cyberspace.* Oxford: Signal.

_____. 2011 "Tracking the emerging arms race in cyberspace". *Bulletin of the Atomic Scientists* 67 (1): 1-8.

Deibert, Ronald J., y Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology*: 15-32.

DeNardis, Laura, y Francesca Musiani. 2016. "Governance by infrastructure". En *The turn to infrastructure in Internet governance*, 3-24. Londres: Palgrave MacMillan.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Cambridge: MIT Press.

DeNardis, Laura, y Mark Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance". *Eighth Annual GigaNet Symposium*, 21 de Octubre.

Diniz, Gustavo, Robert Muggah y Misha Glenny. 2014. "Deconstructing cyber security in Brazil: Threats and responses". Strategic Paper 11: 3-32.

Dunn Cavelty, Myriam. 2012. "The Militarisation of Cyberspace: Why Less May Be

Better". *4th International Conference on Cyber Conflicts*, 141-153.

_____. 2016. "Cyber-security and private actors." Em *Routledge Handbook of Private Security Studies*, Abrahansen, Rita y Anna Leander. eds. Nueva York: Routledge.

_____. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* . London: Routledge.

_____. 2015. "The Normalization of Cyber-International Relations." Em *Strategic Trends 2015: Key Developments in Global Affairs*. CSS.

Dunn Cavelty, Myriam., y Mark Daniel Jaeger. 2015. "(In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous". *International Political Sociology*: 176-194.

Dutton, William H. 2015. "Multistakeholder Internet governance?". *Background Paper: Digital Dividends*.

Epstein, Dmitry, Christian Katzenbach, y Francesca Musiani. 2016. "Doing internet governance: practices, controversies, infrastructures, and institutions". *Internet Policy Review*.

Eriksson, Johan, y Giampero Giacomello. 2009. "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State". *International Studies Review*, 205-230.

Flyverbom, Mikkel. 2016. "Disclosing and concealing: internet governance, information control and the management of visibility". *Internet Policy Review, 30 de septiembre.*

Fontenelle, Alexandre S. 2012. "O Espaço Cibernético na Agenda Internacional". *ECEME, XI Ciclo de Estudos Estratégicos*.

Gonzaga, Alexandre. 2016. "Jungmann apresenta ao presidente Temer a revisão dos documentos de defesa", http://www.defesa.gov.br/noticias/24840-jungmann-apresenta-ao-presidente-temer-a-revisao-dos-documentos-da-defesa.

Hansen, Lene., y Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly*: 1155–1175.

Internet World Stats. 2016. "Internet usage and population in South America", http://www.internetworldstats.com/stats15.htm.

Justribó, Candela. 2014. "Ciberdefensa: una visión desde la UNASUR", http://www.congresos.unlp.edu.ar/index.php/CRRII/CRRIIVII/paper/view/1849/422.

Keohane, Robert., y Joseph Nye. 1998. "Power and Interdependence in the Information Age". *Foreign Affairs* 77 (5): 81-94.

Lee, Stacia. 2017. "The Cybersecurity Implications of Chinese Undersea Cable Investment". *The Henry M. Jackson School of International Studies*.

Lopes, Gills. 2013. "Securitizando o ciberespaço: um estudo comparativo sobre a defesa cibernética em sete países". *4º Encontro Nacional da ABRI.* Belo Horizonte.

Maciel, Marília Ferreira, y Carlos Affonso Pereira de Souza. 2011. "Multi-stakeholder participation on Internet governance: An analysis from a developing country, civil society perspective". *Association for Progressive Communications*.

Maciel, Marilia Ferreira, Nicolo Zingales, y Daniel Fink. 2015. "NoC Internet Governance Case Studies Series: The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) ". *SSRN*.

Mandarino Junior, Raphael, y Claudia Canongia. 2010. *Livro Verde: Segurança Cibernética no Brasil.* Brasília: GSIPR/SE/DSIC.

Ministério da Defesa. 2016a. "Defesa, MRE e GSI aproximam agendas internacionais e criam mecanismo de coordenação", http://www.defesa.gov.br/noticias/26193-defesa-mre-e-gsi-aproximam-agendas-internacionais-e-criam-mecanismo-de-coordenacao.

_____. 2016b. "XII CDMA: Ministro Jungmann defende cooperação regional nas fronteiras", http://www.defesa.gov.br/noticias/25195-xii-cmda-ministro-jugmann-defende-cooperacao-regional-nas-fronteiras.

Mueller, Milton, Andreas Schmidt, y Brenden Kuerbis. 2013. "Internet Security and Networked Governance in International Relations". *International Studies Review*, 86–104.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge: MIT Press.

Mueller, Milton, y Hans Klein. 2014. "Sovereignty, National Security, and Internet Governance: Proceedings of a Workshop". Syracuse University: Georgia Institute of Technology School of Public Policy.

Muggah, Robert, y Thompson Nathan. 2015. "Brazil's Cybercrime Problem". *Foreign Affairs*.

NATO. 2016. "NATO Cyber Defense Fact Sheet", http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology*, 61-73.

Nye, Joseph. 2004. *Power in a global information age: from realism to globalization.* Nueva York: Routledge.

Oppermann, Daniel. 2014. "Internet governance and cyber security in Brazil". En *International Security: a European-South American Dialogue*, 167-182. Río de Janeiro: Konrad-Adenauer-Stiftung.

Portal Brasil. 2015. "Forças Armadas vão monitorar redes de Internet na Rio 2016", http://www.brasil.gov.br/defesa-e-seguranca/2015/09/forcas-armadas-vao-monitorar-redes-de-internet-na-rio-2016.

Rid, Thomas. 2012. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35(1).

Stuenkel, Oliver. 2015. *India-Brazil-South Africa Dialogue Forum (IBSA): The Rise of the Global South?* Londres: Routledge.

Van Eeten, Michel JG., y Milton Mueller. 2012. "Where is the governance in Internet governance?". *New Media & Society*: 720-736.

WSIS. 2005. "Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E.", http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Zakaria, Fareed. 2008. *The Post-American World.* Nova York: W. W. Norton & Company.