A ciberhegemonia dos EUA na OEA

The US cyberhegemony in the OAS

La ciberhegemonía de EEUU en la OEA

Maximiliano Vila Seoane[1]

1. Profesor en la Escuela de Política y Gobierno de la Universidad Nacional de San Martín (UNSAM). Investigador del CONICET. Dr. Phil. por la Universidad de Bremen. E-mail: mvila@unsam.edu.ar
ORCID: 0000-0002-0134-7714

DOI: 10.5752/P.2317-773X.2022v10n4p91-112.

Data de submissão: 23/07/2021
Data de aprovação: 30/05/2023

RESUMO

O artigo propõe o conceito de ciberhegemonia como alternativa ao conceito de ciberpoder. A partir dele, são examinadas as atividades de cibersegurança da Organização dos Estados Americanos (OEA). A julgar pela análise de material primário e secundário, destaca-se que a OEA se estabeleceu como o principal espaço de cooperação em temas de cibersegurança em nível intergovernamental nas Américas, por meio de um conjunto de atividades de assessoria, capacitação e intercâmbio de informações. No entanto, observa-se também que a cooperação tem efeitos adversos para os países latino-americanos. Em primeiro lugar, a OEA reproduz e legitima as ideias para o ciberespaço das forças sociais dos EUA e seus estados aliados. Em segundo lugar, a OEA promove os interesses das empresas de cibersegurança dos Estados Unidos em detrimento das empresas de outros países. Finalmente, a OEA dificulta o questionamento dos ciberataques e da ciberespionagem dos EUA. Consequentemente, conclui-se que a OEA reproduz a ciberhegemonia dos EUA nas Américas.

Palavras-chave: cíbersegurança; ciberhegemonia; ciberpoder; EUA; OEA.

ABSTRACT

This article proposes the concept of cyberhegemony as an alternative to the concept of cyberpower. Based on it, the article examines the cybersecurity activities of the Organization of American States (OAS). Judging by the analysis of primary and secondary sources, it stands out that the OAS has become the main space for cooperation on cybersecurity issues at the intergovernmental level in the Americas, through a set of advisory, training and information exchange activities. However, the article also highlights that these cooperation relations have adverse effects for Latin American countries. First, the OAS reproduces and legitimizes the ideas for cyberspace of the social forces of the US and its allied states. Second, the OAS promotes the interests of US cybersecurity companies over those of companies from other countries. Finally, the OAS hinders challenges to the cyberattacks and cyberespionage activities of the US. Consequently, the article concludes that the OAS reproduces the US cyber hegemony in the Americas.

Keywords: cybersecurity; cyberhegemony; cyberpower; US; OAS.

RESUMEN

El artículo propone al concepto de ciberhegemonía como una alternativa al concepto de ciberpoder. A partir del mismo, se examinan las actividades de ciberseguridad de la Organización de Estados Americanos (OEA). A juzgar por el análisis de material primario y secundario, se destaca que la OEA se estableció como el principal espacio de cooperación en temas de ciberseguridad a nivel intergubernamental en las Américas, mediante un conjunto de actividades de asesoramiento, capacitación e intercambio de información. Sin embargo, también se observa que la cooperación tiene efectos adversos para los países de América Latina. Primero, la OEA reproduce y legitima las ideas para el ciberespacio de las fuerzas sociales de EEUU y de sus Estados aliados. Segundo, la OEA fomenta los intereses de las empresas de ciberseguridad de EEUU sobre los de empresas de otros países. Por último, la OEA obstaculiza el cuestionamiento a los ciberataques y al ciberespionaje de EEUU. Consecuentemente, se concluye que la OEA reproduce la ciberhegemonía estadounidense en las Américas.

Palabras clave: ciberseguridad; ciberhegemonía; ciberpoder; EEUU; OEA.

INTRODUCCIÓN

El avance del proceso de digitalización en nuestras sociedades está multiplicando las amenazas en el ciberespacio. Diariamente nos informamos de nuevos ciberataques, de maliciosas prácticas de cibercrimen, y de preocupantes aumentos de la cibervigilancia, entre otros nuevos desafíos que ilustran los aspectos más problemáticos de la digitalización. Desde la perspectiva de la seguridad internacional, desde los 90s existe una corriente de analistas y pensadores que auguran una inminente ciberguerra a causa de estas nuevas vulnerabilidades (Arquilla; Ronfeldt, 1993; Stone, 2013; Kaplan, 2016). Por el contrario, los críticos a estas posturas belicosas sospechan que la exageración sobre tales potenciales amenazas tal vez se deba al objetivo de asegurar presupuestos para áreas estatales y empresas de ciberseguridad[2] (Rid, 2012; Valeriano; Maness, 2014; Dunn; Tikk; Kerttunen, 2020). Estos autores, más afines a las corrientes liberales y constructivistas de las Relaciones Internacionales, coinciden en señalar que los desafíos de la ciberseguridad no pueden ser enfrentados únicamente desde un abordaje nacionalista y militar, en parte, por las características transnacionales del ciberespacio. Por el contrario, rescatan el imperativo de extender las tradicionales prácticas diplomáticas a los debates en torno a la gobernanza del ciberespacio.

2. Es importante notar que la ciberseguridad es un concepto en disputa, que en su faceta inter- y transnacional abarca una agenda dinámica de temas de gobernanza (KERTTUNEN; TIKK, 2020), que exceden una definición meramente técnica.

En este sentido, y en línea con el consenso en la literatura sobre la importancia de los regionalismos en la gobernanza de temas de seguridad internacional (Kacowicz; Press-Barnathan, 2016), varios organismos regionales, como la OTAN o la ASEAN, han incorporado a la ciberseguridad como un tema prioritario en sus agendas. Nuestro vecindario no ha estado ajeno a estas tendencias. En 2004, la Organización de Estados Americanos (OEA) fue pionera en establecer una estrategia de ciberseguridad a nivel regional (OEA, 2004). Más recientemente, otras iniciativas regionales, como la UNASUR y la CELAC, incorporaron a la ciberseguridad como un tema de sus agendas, pero ninguna de ellas la impulsó tanto como la OEA. A pesar de esto, sólo

un par de estudios realizaron una mención breve y superficial sobre la ciberseguridad en la OEA (Sancho, 2017; Castro; Moneteverde, 2018). Ante este vacío de conocimiento, el objetivo de este artículo es examinar las actividades de ciberseguridad de la OEA por intermedio del estudio de los actores que impulsaron el tema en su agenda, sus cambios a lo largo del tiempo, y los aspectos problemáticos de la iniciativa para los Estados miembro. El artículo está basado en el análisis de material primario y secundario de las actividades del programa de ciberseguridad de la OEA entre 2004-2020, recolectadas tanto de fuentes online como de la observación participante del autor en eventos de ciberseguridad organizados por la OEA.

En el artículo se sostiene que la OEA reproduce la ciberhegemonía de EEUU en las Américas. En efecto, el análisis muestra que la OEA se ha establecido como el principal espacio de cooperación regional en temas de ciberseguridad a nivel intergubernamental mediante un conjunto de actividades de asesoramiento, capacitación e intercambio de información entre sus Estados miembro. Sin embargo, el material empírico también indica que la cooperación, aparentemente benévola y consensual, tiene al menos tres efectos adversos para los países de América Latina. Primero, la OEA reproduce y legitima las ideas de las fuerzas sociales de EEUU para el ciberespacio, y en menor medidas, de las de sus Estados aliados. Segundo, la OEA fomenta los intereses de las empresas de ciberseguridad de EEUU sobre los de empresas de otros países. Por último, a diferencia de los patrones de coordinación de políticas de ciberseguridad que se observan en la Unión Europea o en la ASEAN, la OEA obstaculiza el cuestionamiento a los ciberataques y al ciberespionaje de EEUU en el ciberespacio.

Este argumento se desarrolla en cuatro secciones. En la primera se introducen los conceptos de ciberhegemonía y de ciberpoder. En la segunda se sintetiza el debate sobre el rol de EEUU en la OEA. En la tercera se realiza un análisis del programa de ciberseguridad de la OEA, seguido de una cuarta sección que explora sus efectos adversos.

CIBERPODER Y CIBERHEGEMONÍA

Tras introducir y criticar el concepto de ciberpoder, esta sección presenta como alternativa al concepto de ciberhegemonía, que está inspirado en un enfoque de economía política internacional crítica.

El concepto de ciberpoder ha sido propuesto en la literatura para comprender cómo el ciberespacio ofrece nuevas formas de proyección de poder estatal (Dunn, 2018) Entre la.s variantes existentes sobre este concepto, Betz y Stevens (2011, p. 44) entienden al ciberpoder como "[…] la manifestación del poder en el ciberespacio más que una forma nueva o diferente de poder". En particular, los autores postulan que el ciberpoder tiene cuatro dimensiones. La primera la titulan ciberpoder compulsivo, y abarca el uso directo de coerción por parte de un actor hacia otro con el fin de cambiar sus acciones (Betz; Stevens, 2011, p. 45). Los ciberataques y la movilización de recursos simbólicos, como amenazas de sanciones o de un ataque militar en respuesta a incidentes en el ciberespacio, son

ejemplos de esta dimensión. La segunda es el ciberpoder institucional, entendido como el control indirecto de un actor sobre otro por intermedio de la influencia en instituciones intermediarias. Por ejemplo, Betz y Stevens (2011, p. 47) citan cómo EEUU promueve las normas para el ciberespacio en organizaciones internacionales. La tercera dimensión es el ciberpoder estructural, que engloba cómo las características del ciberespacio afectan las posiciones relativas de los actores en las estructuras de poder preexistentes. Según Betz y Stevens (2011, p. 50), un ejemplo de ciberpoder estructural es como la estructura transnacional de las redes sociales propició la Primavera Árabe. La última dimensión se denomina ciberpoder productivo, e incluye cómo los discursos que circulan en o sobre el ciberespacio moldean subjetividades y definen los límites de lo posible en términos de acción social. Según Betz y Stevens (2011, p. 51), esta quizás sea la dimensión más importante de las cuatro. A modo de ilustración, mencionan la construcción discursiva y sesgada que distintos actores estatales y empresas realizan sobre las amenazas existentes en el ciberespacio.

En síntesis, el enfoque conceptual de Betz y Stevens incluye tanto dimensiones que entienden al poder como un recurso, como así también dimensiones que lo entienden de una forma más bien relacional y difusa (Dunn, 2018, p. 5). No obstante, para los fines de este artículo, el concepto tiene al menos tres debilidades que precisan ser subsanadas. En primer lugar, no ofrece un marco explicativo para entender porqué algunos actores del sistema internacional tendrían más ciberpoder que otros. Esto es producto de pensar el concepto de forma abstracta sin considerar las trayectorias históricas desiguales en la acumulación de capacidades en el ciberespacio, y en particular en ciberseguridad, donde los actores de EEUU tienen una ventaja considerable (Vila Seoane; Saguier, 2019). En segundo lugar, si bien Betz y Stevens (2011, p. 43) afirman que el ciberpoder es movilizado por un actor para fines estratégicos, en su elaboración conceptual no realizan ninguna vinculación explícita con otras teorías que expliquen cuáles podrían ser tales objetivos. Por último, si bien la definición de ciberpoder institucional es relevante para los fines de este artículo, dice poco sobre cómo se realiza dicha influencia.

Como alternativa, en este artículo se define a la ciberhegemonía como la extensión del concepto de hegemonía de Cox para el ciberespacio. Para explicar esta ampliación, es preciso recordar las especificidades de este concepto de hegemonía de inspiración gramsciana. A diferencia del realismo, que suele entender a la hegemonía como una relación de dominación entre Estados, el concepto de hegemonía propuesta por Cox (1981; 1983) es una relación principalmente de influencia consensual de un conjunto de fuerzas sociales sobre otras, aunque sin excluir el uso potencial de acciones coercitivas (Cox, 1983), que están siempre latentes y que pueden ser empleadas en casos particulares. En sus trabajos, Cox extendió el concepto de hegemonía de Gramsci para explicar los cambios en las estructuras hegemónicas mundiales. Según Cox (1981, p. 136), una estructura hegemónica mundial es histórica y está sostenida por un conjunto de ideas, instituciones y capacidades materiales. Las capacida-

des materiales incluyen a las capacidades tecnológicas y organizacionales. El concepto de ideas, abarca los significados intersubjetivos que influencian y reproducen formas de acción social. Cox también incluye en este concepto a las diferentes visiones en disputa sobre el orden mundial que mantienen distintas fuerzas sociales entre sí. Por último, con instituciones Cox alude a una combinación de capacidades materiales e ideas, que coadyuvan a estabilizar y mantener un dada estructura hegemónica mundial (Cox, 1981, p. 137). Por ejemplo, las organizaciones internacionales pueden ser consideradas como mecanismos que reproducen las reglas de una estructura hegemónica mundial, lo legitiman ideológicamente, cooptan ideas de las elites de países periféricos y las ideas contrahegemónicas que lo puedan llegar a desafiar (Cox, 1983, p. 172). Adicionalmente, Cox sostiene que si bien la participación en estas instituciones puede transferir elementos de modernización a los países periféricos, sólo lo hacen en línea con los intereses de los actores que impulsan la estructura hegemónica mundial (Cox, 1983, p. 173). En definitiva, estos conceptos heurísticos pueden trasladarse a las discusiones sobre el ciberespacio si definimos que una estructura ciberhegemónica mundial es histórica y está sostenida por un conjunto de ideas, instituciones y capacidades materiales que se expresan dentro del ciberespacio, o por fuera de él, a fines de moldear el orden en el ciberespacio.

Cabe notar que existe un solapamiento entre las propuestas conceptuales de Cox (1983) y las de ciberpoder postuladas por Betz y Stevens (2011). Por ejemplo, el uso de capacidades materiales en el ciberespacio con fines coercitivos sería equivalente al ciberpoder coercitivo. Por su parte, la dimensión institucional de Cox incluye a la dimensión de ciberpoder institucional de Betz y Stevens, pero la excede, ya que también considera la materialidad que sustenta la mayor influencia de un conjunto de ideas sobre otras en estos ámbitos. El concepto de ideas contiene la dimensión de ciberpoder productivo. No obstante, el concepto de ciberhegemonía responde a las debilidades mencionadas previamente sobre el concepto de ciberpoder. Por un lado, se puede entender que las fuerzas sociales de los Estados a la vanguardia de la digitalización tienen ventaja en internacionalizar sus acciones y preferencias sobre el ciberespacio (Vila Seoane; Saguier, 2019). Además, el concepto de fuerzas sociales abarca distintas configuraciones de actores estatales y no estatales, incluyendo a las empresas multinacionales, generalmente en línea—aunque no siempre—con sus Estados de origen. Por otro lado, desde este marco analítico se puede entender que el fin de las estrategias de ciberhegemonía es influir en las distintas estructuras de gobernanza del ciberespacio con el objetivo de moldear y reproducir una determinada estructura ciberhegemónica mundial.

En síntesis, este trabajo propone extender el clásico concepto de hegemonía de Cox al ciberespacio como alternativa al concepto de ciberpoder. Esta conceptualización de ciberhegemonía, que entiende a las organizaciones internacionales como mecanismos de un estructura ciberhegemónica mundial, se emplea en el resto del artículo para analizar cómo distintas fuerzas sociales influenciaron la agenda de ciberseguridad en la OEA.

LA OEA, EEUU Y LAS AMÉRICAS

Antes de abordar las iniciativas específicas sobre ciberseguridad de la OEA, esta sección presenta una breve síntesis de antecedentes importantes sobre este organismo, que contextualizan el rol de la institución como vehículo para la proyección de hegemonía de EEUU en las Américas.

Creada en 1948 en Colombia, y con sede en Washington DC, la OEA es el organismo regional más antiguo del mundo que junta a los 35 Estados del continente americano. Según la Carta de la OEA, su principal propósito es afianzar la paz y la seguridad del continente, seguido por la promoción y la consolidación de la democracia representativa. En cuanto a su funcionamiento, cabe destacar a la Asamblea General, que es el órgano supremo que define las políticas y mandatos de la organización, donde cada Estado tiene derecho a un voto, independientemente de su población o del aporte financiero que realiza al organismo. La Secretaría General ejecuta las funciones que la Carta de la OEA y que otros tratados le asignan, y es liderada por un Secretario General elegido por la Asamblea General. Por último, es importante mencionar que la OEA tiene la potencialidad de extender sus funciones al crear nuevas entidades y organismos especializados que aborden temas de interés para los Estados miembro.

En las Américas, la OEA es una organización polémica debido a que EEUU la instrumentalizó en repetidas ocasiones para avanzar sus objetivos de política exterior. Esta tendencia fue notoria durante la Guerra Fría (Herz, 2008; López, 2009; Weiffen, 2012). Por ejemplo, en 1962, la OEA suspendió a Cuba bajo el argumento de que las influencias extrarregionalas sobre la isla (en referencia a la Unión Soviética), junto a la ideología Marxista-Leninista, constituían una amenaza a los sistemas democráticos de la región (OEA, 1962). No obstante, la declaración nada dijo de las dictaduras anticomunistas y conservadoras en su propio seno (López, 2009), exponiendo así el evidente alineamiento de la OEA con EEUU. Sin embargo, esta influencia sobre los países de América Latina en la OEA nunca fue total. De hecho, en las últimas dos décadas de la Guerra Fría se acentuaron las diferencias de los países de la región con EEUU, y en 1975, incluso se acordó la libertad de acción de cada país en cuanto a sus vínculos con Cuba (Herz, 2008; López, 2009).

Tras la disolución de la Unión Soviética, y el auge de la unipolaridad de EEUU, se aceleró un proceso global de redefinición de amenazas de seguridad, que mutaron de las estrictamente militares y estadocéntricas a todo un nuevo abanico de amenazas transnacionales no tradicionales (Kacowicz; Press-Barnathan, 2016). En este contexto de post-Guerra Fría, la OEA adoptó el concepto de seguridad cooperativa, que contribuyó a disminuir tensiones interestatales, e impulsó de forma incipiente la conformación de una comunidad de seguridad (Thérien; Mace; Gagné, 2012; Weiffen, 2012). En 2003, la OEA inició una nueva agenda para la seguridad multidimensional (OEA, 2003b), que extendió el concepto de seguridad al abarcar un abanico heterogéneo de amenazas, como el terrorismo, el crimen transnacional organizado, la pobreza extrema, y la seguridad cibernética, entre otras (OEA, 2003b, p. 4).

Sin embargo, tras los atentados del 11 de Septiembre de 2001, los documentos priorizaron al terrorismo y al narcotráfico (Weiffen, 2012; Weiffen; Wehner; Nolte, 2013). Esto conformó un nuevo giro hacia una perspectiva más de defensa colectiva en línea con las prioridades de EEUU y su Guerra Global contra el Terrorismo. Consecuentemente, se incrementó la desconfianza de varios Estados de la región ante una nueva instrumentalización de la OEA por parte de EEUU. No obstante, esto no significó un retorno al período de la Guerra Fría, ya que el giro a la izquierda de varios gobiernos de la región propició la elección de un Secretario General progresista (2005-2015), José Miguel Insulza, que por primera vez en la historia de la OEA, no fue el candidato favorito de EEUU.

A pesar de estas excepciones, persiste una suspicacia histórica hacia la organización por parte de los partidos de tendencia progresista en América Latina, que emanan de un conjunto de factores estructurales. En primer lugar, el financiamiento del organismo depende de EEUU, hecho que le permite influenciar de manera notoria las agendas de la OEA[3]. En segundo lugar, hay prioridades diferentes entre los Estados miembros. Mientras que el foco de la mayoría de los países de América Latina suele estar en el desarrollo económico y social, la agenda de EEUU, con Canadá generalmente alineada, responde a temas de seguridad (Herz, 2008, p. 25). En tercer lugar, persisten diferencias considerables en torno a varios temas, por ejemplo, sobre el tipo de vinculación a establecer con Cuba, sobre cómo abordar el problema del narcotráfico, y sobre el posicionamiento respecto a la cuestión de las Islas Malvinas (Thérien; Mace; Gagné, 2012, p. 159). Por último, los críticos de la OEA entienden que la elección de Luis Almagro como Secretario General en 2015 reintrodujo una agenda alineada con la superpotencia del Norte (Long, 2020). Esto fue especialmente evidente en la postura de la OEA contraria a Venezuela, y en la deslegitimación de las elecciones de 2019 en Bolivia.

En síntesis, la OEA es el principal organismo de cooperación internacional a nivel interamericano. Sin embargo, la influencia y las recurrentes intervenciones de EEUU para avanzar su política exterior en la región por intermedio de la OEA, en otras palabras, la reproducción de su hegemonía por intermedio de la OEA, la convierten en un organismo internacional polémico. Esto explica las iniciativas de los gobiernos progresistas de América Latina de construir organizaciones y mecanismos regionales de cooperación contrahegemónicos, que deliberadamente excluyen de su membresía a EEUU y Canadá, como la UNASUR o CELAC (Weiffen; Wehner; Nolte, 2013). Es en este contexto que hay que situar el surgimiento y desarrollo de la agenda y de las prácticas de ciberseguridad de la OEA.

LA OEA Y LA CIBERSEGURIDAD

La incorporación del tema de ciberseguridad en la agenda de la OEA está estrechamente vinculada a las nuevas prioridades de la política exterior de EEUU. Tras los ataques terroristas de 2001, en EEUU se acentuaron los miedos sobre potenciales ciberataques devastadores contra sus infraestructuras críticas, que impulsaron la publicación de la primera es-

3. Según el presupuesto aprobado en 2021, EEUU contribuyó con el 59,4% del total de 89,770,207 US$ asignados para el fondo regular del organismo. Brasil fue el segundo país con más aportes (12,7%), seguido por Canadá (9,7%), mientras que el aporte de los 31 países restantes representó el 18,1% del total.

trategia nacional para asegurar el ciberespacio (The White House, 2003). Este documento de la administración Bush tuvo como objetivo principal la prevención de ciberataques, y en caso de padecerlos, minimizar los posibles daños y reducir el tiempo de recuperación (The White House, 2003, p. 14). Para alcanzar estos fines, la Casa Blanca se propuso incrementar la cooperación internacional, incluyendo la creación de comités responsables de temas de ciberseguridad en organizaciones regionales, como la OEA (The White House, 2003, p. 51).

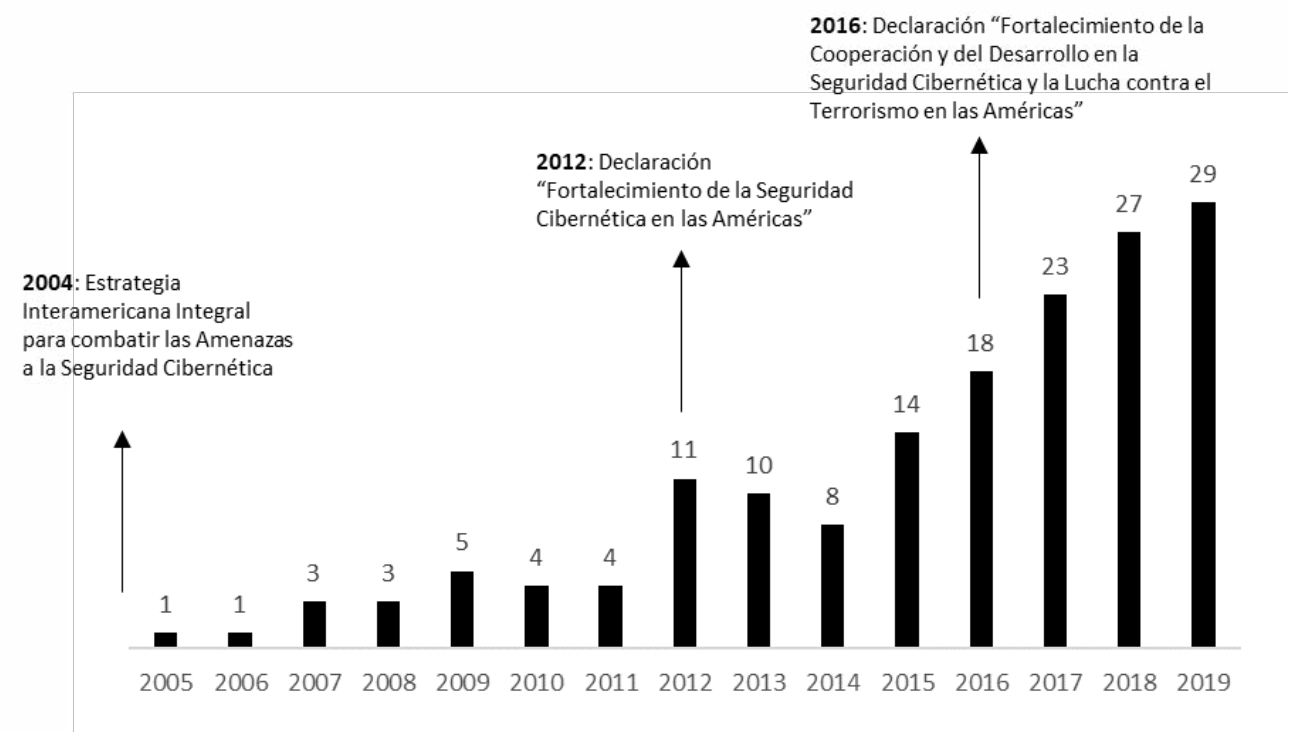
En este contexto, en 2004, la Asamblea General de la OEA aprobó la denominada Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética (OEA, 2004), donde los Estados miembro se comprometieron al desarrollo de una cultura de ciberseguridad en la región, que evite los riesgos del uso de Internet. De las entidades de la OEA que recibieron el mandato para asistir a los Estados miembros en temas de seguridad cibernética, el Comité Interamericano contra el Terrorismo (CICTE), ha sido la de mayor visibilidad. Por ende, la siguiente sección se focaliza en el estudio de las actividades de ciberseguridad de CICTE.

CICTE

CICTE fue propuesto por la Asamblea General en 1999 con el fin de "[…] prevenir, combatir y eliminar los actos y actividades terroristas" (OEA, 1999, p. 4). Si bien originalmente la ciberseguridad no estaba en sus temáticas, sí se incorporó en la declaración de San Salvador de enero de 2003, aunque con el término de 'seguridad cibernética' (OEA, 2003a). Meses más tarde, esta asociación entre el terrorismo y la ciberseguridad figuró de nuevo en la Declaración sobre Seguridad en las Américas, donde los países miembros identificaron a los ataques a la seguridad cibernética como una amenaza terrorista emergente a la par de los ataques dirigidos a infraestructuras críticas y ataques biológicos (OEA, 2003b, p. 9). Tras recibir el mandato en temas de seguridad cibernética, CICTE incorporó actividades de ciberseguridad en sus planes de trabajo anuales[4] y realizó declaraciones anuales específicas sobre ciberseguridad. En función de estos documentos, se pueden clasificar las acciones de ciberseguridad de este comité en los siguientes tres períodos: 2004-2011, 2012-2015 y 2016-2020.

4. Los documentos se obtuvieron de http://www.oas.org/en/sms/cicte/events_sessions.asp

Gráfico 1 - Cantidad de actividades de ciberseguridad de CICTE planeadas por año[5]



Fuente: Elaboración propia en base a los planes anuales de trabajo de CICTE[6].

5. El número de actividades por año incluye a los distintos ítems incluidos en cada plan anual de trabajo.

6. El año 2020 fue excluido, pues sólo se informan resultados a alcanzar en vez de actividades a realizar como en años previos, posiblemente por las limitaciones a causa de la pandemia.

2004-2011

Desde 2004 a 2011, la principal actividad de CICTE fue dinamizar una red de centros de respuesta a incidentes en seguridad cibernética (OEA, 2004), o CSIRTs por sus siglas en inglés. El objetivo fue impulsar la creación de al menos un centro por país para que intercambien información sobre amenazas y vulnerabilidades en Internet a nivel nacional e internacional, con el fin de recuperarse velozmente ante incidentes de ciberseguridad. Durante estos años, CICTE también empieza a organizar—aunque de forma embrionaria—los primeros talleres de capacitación en ciberseguridad, por ejemplo, en contra del delito informático.

Durante estos años, los informes de CICTE revelan un esfuerzo retórico frecuente en asociar las amenazas de ciberseguridad con el terrorismo. Por ejemplo, en varias de las declaraciones anuales se menciona la necesidad de combatir a las amenazas terroristas emergentes, entre las cuales se destaca el "[…] delito cibernético y bio-terrorismo y las amenazas a la seguridad en el turismo y la infraestructura critica" (CICTE, 2006, p. 8). Dado el foco de CICTE en temas de terrorismo, es entendible que los documentos del comité comprendieran a las amenazas de ciberseguridad como terroristas. Sin embargo, es importante notar que la introducción del tema en la agenda de CICTE estuvo evidentemente influenciada por las preferencias normativas que en su momento tenía EEUU. En efecto, en el marco de la Guerra Global contra el Terrorismo, la estrategia de ciberseguridad del Presidente Bush situó a los terroristas como uno de

los principales actores maliciosos detrás de ciberataques, a la par de las amenazas de otros Estados, criminales e individuos (The White House, 2003, p. 27). A su vez, la estrategia de ciberseguridad de EEUU expresó la decisión deliberada de utilizar a los organismos internacionales patrocinados por el Estado, incluyendo a la OEA, para coordinar posiciones comunes en ciberseguridad (The White House, 2003, p. 51). El motivo fue el supuesto de que la mayoría de los ciberataques que enfrentaba el Estado, los mercados financieros y las empresas de EEUU provenían del exterior, por ende, se precisaba de la cooperación internacional para enfrentarlos (The White House, 2003, p. 51). En definitiva, por intermedio de la OEA, EEUU empezó a proyectar sus ideas para el ciberespacio en las Américas.

2012-2015

Este período inició con la declaración sobre el 'Fortalecimiento de la Seguridad Cibernética en las Américas' (OEA, 2012a), donde los Estados miembro se comprometieron a revitalizar los esfuerzos iniciados en 2004. Desde entonces, se incrementaron considerablemente las actividades de CICTE en apuntalar las capacidades en ciberseguridad de los Estados miembro (Ver Gráfico 1). En el informe anual de actividades de 2012, CICTE reporta la realización de misiones de apoyo técnico a 14 países y la capacitación de más de 770 oficiales de la región (OEA, 2013a). Entre 2012-2015, CICTE asesoró a países en el diseño de sus propias estrategias nacionales de ciberseguridad, entre ellos: Colombia, Paraguay y Trinidad y Tobago. Adicionalmente, CICTE incrementó la organización de cursos, seminarios y talleres de capacitación en temas de ciberseguridad (OEA, 2013a; 2014; 2015a).

En este período se ampliaron los esfuerzos de funcionarios de EEUU en influenciar las discusiones en torno a la gobernanza de Internet en general, y de la ciberseguridad en particular. Por ejemplo, en la sesión plenaria de 2012, como es costumbre, participaron funcionarios de la OEA y los embajadores de los Estados miembro, junto a distintos funcionarios y representantes de empresas de EEUU. De los oradores, cabe destacar la alocución de Christopher Painter, que era el coordinador de ciberasuntos del Departamento de Estado de EEUU. Por un lado, Painter sintetizó los avances realizados por la OEA en ciberseguridad (OEA, 2012b), y subrayó la importancia de consensuar normas y principios en común para la gobernanza del ciberespacio. Por ejemplo, la preservación de libertades fundamentales, el respeto a la propiedad privada, la protección del derecho a la privacidad, el compromiso a mantener la estabilidad de la red, entre otros temas (OEA, 2012b). Todas ideas en línea con las prioridades de la nueva estrategia de ciberseguridad de la administración Obama de la que Painter formaba parte (The White House, 2011).

Por otro lado, el llamado de Painter a buscar el consenso en el ciberespacio se realizó a la par de una caracterización maniquea de otros Estados que no comparten las normas impulsadas por EEUU. Por ejemplo, sin mencionarlos explícitamente, Painter dijo que tales Estados abogan por un mayor control del comercio impulsado por Internet y del contenido online por considerarlos como una amenaza a la estabilidad políti-

ca y social de sus países (OEA, 2012b, p. 6). Igualmente, alegó que tales Estados suelen renegar de las normas para el ciberespacio para facilitar actividades consideradas por otros como criminales (OEA, 2012b, p. 6). Este tipo de intervenciones ejemplifican como los funcionarios de EEUU en la OEA utilizan este espacio de cooperación para difundir ideas sobre con qué actores es bueno cooperar en ciberseguridad, y con cuáles una amenaza.

Aparte de la presencia de funcionarios de EEUU, en estos años se inició una articulación entre CICTE y otras fuerzas sociales estadounidenses y de Estados aliados. En particular, se destacan las empresas de tecnología de EEUU con capacidades en ciberseguridad. Por ejemplo, en 2014, CICTE publicó un informe en conjunto con la empresa estadounidense Symantec sobre las brechas de ciberseguridad en las Américas (OEA; Symantec, 2014), y en 2015, otro con la empresa Trend Micro que examina el riesgo de los sistemas industriales de la región ante ciberataques (OEA; Trend Micro, 2015). CICTE también estableció convenios de cooperación con Microsoft para incrementar las capacidades de ciberseguridad de los Estados miembro. De forma similar, CICTE inició la construcción de alianzas con otros actores, como el BID, el Foro Económico Mundial y la Universidad de Oxford, a fin de avanzar con su agenda de ciberseguridad en la región (OEA, 2015a). El denominador común de estos casos es que son actores no estatales de EEUU, de aliados u otros organismos donde EEUU tiene considerable influencia financiera y política.

Por último, si bien en las declaraciones anuales de CICTE persistió la asociación entre terrorismo y ciberseguridad (OEA, 2015b, p. 7), en la práctica, las actividades estuvieron orientadas a influenciar normativamente a los Estados miembro sobre la gobernanza de la ciberseguridad y en ofrecer capacitaciones para enfrentar ciberataques, independientemente de si tienen o no un origen terrorista. Posiblemente esto estuvo vinculado con el hecho de que el terrorismo ya no ocupaba un lugar preponderante en la estrategia de ciberseguridad de Obama. De hecho, este documento sólo menciona al terrorismo una vez en contraposición a las nueve veces que figuró en la estrategia previa de Bush (The White House, 2003; 2011).

2016-2020

El último período estuvo influenciado por cambios tanto en la OEA como a nivel regional que acontecieron a partir de 2015. En mayo de ese año, la OEA escogió a un nuevo secretario general, Luis Almagro, que en poco tiempo alineó a la organización con las prioridades de política exterior de EEUU (Long, 2020). A partir de 2016, varios países de la región eligieron a presidentes de orientación política de centroderecha o extrema derecha, como en Argentina, Brasil, Chile, etc., que debilitaron procesos previos de integración regional contrahegemónicos, como la UNASUR. Esto cercenó los esfuerzos incipientes en generar una doctrina regional en ciberdefensa en ese ámbito (Aranda; Riquelme; Salinas, 2015). En 2017, la llegada de Donald Trump a la presidencia de EEUU aceleró los procesos de fragmentación a nivel regional. Ante esta coyuntura regional, y

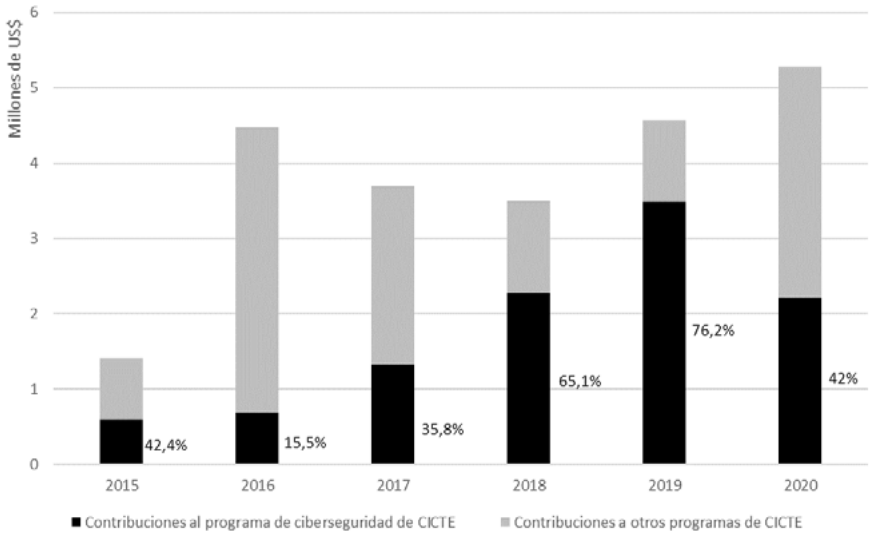
ante una creciente demanda de capacitación en temas de ciberseguridad, CICTE encontró un escenario incluso más propicio que en el período previo para expandir sus actividades.

En efecto, el período inicia con la declaración anual de CICTE titulada 'Fortalecimiento de la Cooperación y del Desarrollo en la Seguridad Cibernética y la Lucha contra el Terrorismo en las Américas' (OEA, 2016), donde se repitieron los compromisos previamente asumidos en esta temática. En el evento expusieron representantes de distintas fuerzas sociales de EEUU, como el Departamento de Estado, la división del FBI dedicada a asuntos cibernéticos, Microsoft, y un académico del think tank Center for Strategic and International Studies (CSIS). El coordinador de ciberasuntos del Departamento de Estado, Christopher Painter, reafirmó el interés de EEUU en continuar apoyando las capacidades de ciberseguridad en las Américas, y en construir un régimen de ciberestabilidad a nivel internacional, a fin de cooperar ante amenazas comunes y evitar los conflictos en el ciberespacio (Painter, 2016, p. 4).

Asimismo, durante estos años se multiplicaron las actividades del período previo, como los cursos de capacitación, talleres y seminarios. También la OEA extendió su asesoramiento en la elaboración de estrategias de ciberseguridad nacional a otros países (OAS, 2017; OEA, 2020a), con una participación más activa de aquellos gobernados por partidos de derecha, como Argentina, Brasil y Chile. Adicionalmente, se añadieron nuevas acciones, como la intención de establecer medidas de fomento de la confianza que limiten las chances de conflicto en el ciberespacio (OEA, 2016).

La importancia que cobró la ciberseguridad se puede ver en el aumento del presupuesto asignado a este programa de CICTE. Cabe recordar que los programas de la OEA se financian por intermedio de fondos regulares y de fondos específicos. Los primeros provienen de los aportes de cada uno de los Estados miembro, con contribuciones mayoritarias de EEUU, mientras que los segundos son las contribuciones voluntarias de Estados miembro, Estados observadores y de otros actores no estatales. La OEA sólo publica los fondos específicos de forma desagregada por programa. Estos datos son los que se observan en el Gráfico 2, y que muestran el progresivo aumento del presupuesto asignado al programa de ciberseguridad de CICTE, salvo en 2020, donde, por causa de la pandemia, se incrementaron las contribuciones a su programa de bioseguridad.

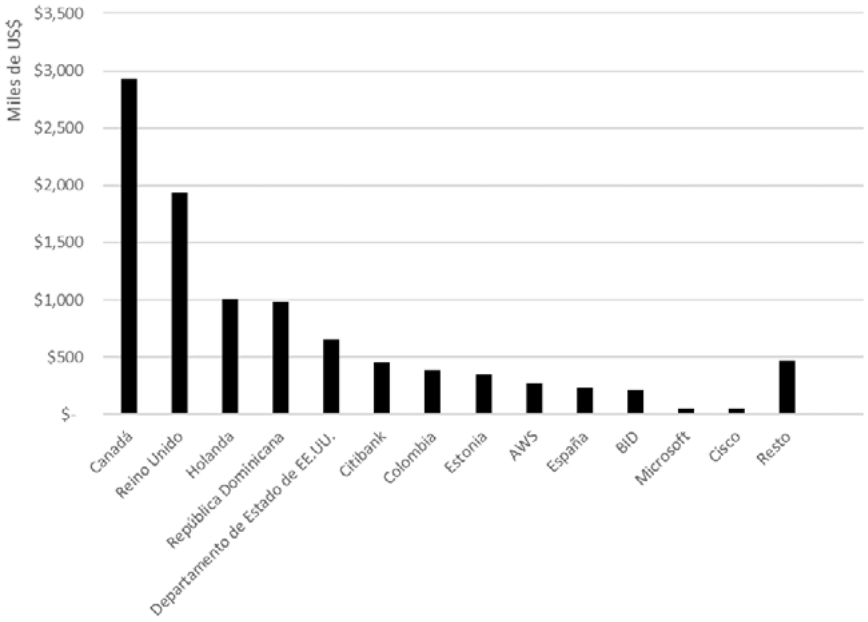
Gráfico 2 - Fondos específicos por año del programa de ciberseguridad versus otros programas de CICTE



Fuente: elaboración propia en base a datos públicos de la OEA.

Durante estos años, CICTE consolidó el financiamiento que recibió de parte de otros gobiernos (OEA, 2020a). En efecto, en el Gráfico3 se desglosa quiénes realizaron las contribuciones a los fondos específicos del programa de ciberseguridad de CICTE entre 2016-2020. De la región, Canadá fue el país que más aportó, seguido por República Dominicana, el Departamento de Estado de EEUU y Colombia. También hay que mencionar el financiamiento del BID. En cuanto a Estados fuera de la región, Reino Unido fue el país que más aportó, seguido de Holanda, Estonia y España. El resto de las contribuciones del gráfico fueron realizadas por empresas de EEUU, como el Citibank, AWS, Microsoft y Cisco.

Gráfico 3 - Contribuciones totales por patrocinador realizadas entre 2016-2020 al fondo específico del programa de ciberseguridad de CICTE



Fuente: elaboración propia en base a datos públicos de la OEA.

Esto tuvo su correlato en la organización de actividades de la OEA en conjunto con estos países. Por ejemplo, la iniciativa denominada Summer Bootcamp, impartida por el Instituto Nacional de Ciberseguridad de España, y la participación y asesoramiento de especialistas de Estonia en eventos de la OEA. Si bien se podría pensar que estos ejemplos ilustran la apertura de la OEA a influencias de otros Estados extrarregionales, el denominador común de estos financistas es que son miembros de la OTAN, la alianza militar liderada por EEUU. Por ende, no desafían la ciberhegemonía que EEUU pretende mantener en el ciberespacio.

Por último, la importancia que adquirió la problemática de la ciberseguridad a nivel regional también derivó en que varios países establecieran acuerdos o convenios con la OEA para recibir asesoramiento específico. Cabe destacar el caso de Colombia, el país que más colaboró con CICTE en ciberseguridad. Estos vínculos fluidos se pueden interpretar como una extensión de su estrecha e histórica cooperación en seguridad con EEUU. Por ejemplo, en 2016 la OEA acordó la elaboración de un estudio sobre los impactos de los ciberataques en Colombia, cuyo resultado fue publicado con el BID. La OEA procuró establecer esta experiencia como un modelo de trabajo a replicar en otros países de la región (Garcinuño, 2016). Igualmente, en 2019, el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia suscribió un convenio con la OEA para vigorizar sus capacidades en ciberseguridad.

En resumidas cuentas, esta síntesis de los tres períodos de CICTE coincide con la apreciación de Contreras y Barrett (2020, p. 215), funcionarios del programa de ciberseguridad de la OEA, que opinaron que la organización, "[…] se ha consolidado como un centro de intercambio de

información sobre amenazas de seguridad cibernética y es una fuente de referencia para América Latina y el Caribe". Incluso en los años en los que aún operaba la UNASUR, la OEA fue el ámbito por excelencia para la cooperación en ciberseguridad a nivel intergubernamental. Desde 2004, las actividades realizadas por la OEA han pasado de ser un proyecto marginal atado a la Guerra Global contra el Terrorismo de EEUU, a convertirse en el programa insignia de CICTE.

A pesar de estos esfuerzos, los desafíos que enfrenta la OEA para cumplir su misión de fortalecer a la ciberseguridad en la región son considerables. Según Contreras y Barrett (2020, p. 216), la ciberseguridad no es aún una prioridad en la mayoría de los países, y por ende, no se le asignan fondos suficientes. Además, son pocos los países que cuentan con formación especializada en ciberseguridad, y peor aún, muchas empresas aún carecen de planes para defenderse de ciberataques (Contreras; Barrett, 2020). No obstante, esta autocrítica de los funcionarios de la OEA poco dice de las contradicciones y sesgos del programa, aspectos que se examinan a continuación.

EFECTOS ADVERSOS DE LA CIBERHEGEMONÍA DE EEUU EN LA OEA PARA LOS PAÍSES DE AMÉRICA LATINA

La cooperación aparentemente benévola y consensual en el área de ciberseguridad en el marco de la OEA omite al menos tres efectos adversos para los países de América Latina. A saber, la OEA reproduce y legitima las ideas para el ciberespacio de las fuerzas sociales de EEUU. y de sus Estados aliados, fomenta los intereses de las empresas de ciberseguridad de EEUU, y obstaculiza el cuestionamiento a los ciberataques y al ciberespionaje de EEUU en el ciberespacio.

Reproduce y legitima las ideas para el ciberespacio de las fuerzas sociales de EEUU y de sus Estados aliados

Los funcionarios de la OEA suelen afirmar que la organización se ha convertido en el principal centro de intercambio de información sobre ciberamenazas de la región (Contreras; Barrett, 2020, p. 215), pero no pareciera ser un centro muy objetivo. Más bien prioriza un intercambio de información asimétrico, que tiende a reproducir y legitimar las ideas sobre ciberseguridad que pregonan las fuerzas sociales estadounidenses y las de sus Estados aliados.

Esto fue evidente desde el inicio del programa de ciberseguridad de CICTE, que asoció a la ciberseguridad con el terrorismo. Si bien la región no ha estado exenta de repudiables actos de terrorismo, este no era ni es el concepto más pertinente para entender los desafíos de seguridad que enfrentan el resto de los países de las Américas (Herz, 2008, p. 26). La ciberseguridad no es la excepción, pues nunca hubo un ataque terrorista por medios cibernéticos en países latinoamericanos, por ende, se trató de una asociación arbitraria, permeada por la práctica de construcción de amenazas de EEUU en el marco de su Guerra Global contra el Terrorismo (Dunn, 2008). Sólo la República Bolivariana de Venezuela objetó—con poco éxito—el vínculo espurio entre amenazas emergentes y terrorismo (CICTE, 2006, p. 9; OEA, 2007, p. 17).

Asimismo, en cuanto a los oradores en los eventos organizados por CICTE, se destacó la presencia de funcionarios de distintas agencias del gobierno de EEUU vinculadas a la ciberseguridad, y en menor medida, académicos y miembros de organizaciones civiles relacionadas a Internet con base en la superpotencia. También participaron especialistas de otros países de la OTAN que financiaron el programa, como expertos de Canadá, el Reino Unido, España y Estonia. De esta forma, las fuerzas sociales de EEUU, secundadas por las de sus aliados de la OTAN, procuraron legitimar su visión para el ciberespacio y cooptar a las elites de los países de América Latina.

A su vez, los documentos elaborados por la OEA suelen suponer que el conocimiento sobre ciberseguridad sólo se encuentra en el puñado de países Occidentales más avanzados económica- y tecnológicamente que financian el programa. El supuesto es que estos Estados, sus empresas y especialistas sí pueden analizar, diagnosticar y recomendar políticas públicas a los Estados con menores capacidades del Sur, por más que conozcan poco sobre estos países. Además, la relación contraria está ausente. Un ejemplo de esta asimetría en la producción de conocimiento es el informe sobre ciberseguridad elaborado entre el BID y la OEA (2016), que promete realizar un diagnóstico sobre la situación de la seguridad cibernética en la región. Para ello, adopta un marco conceptual elaborado por el Centro Global de Capacidad sobre Seguridad Cibernética de la Universidad de Oxford y lo aplica a casi todos los prestatarios del banco en la región. De forma similar, la bibliografía de un artículo sobre el programa de ciberseguridad de la OEA, que fue elaborado por sus funcionarios, hace referencia mayoritariamente a think tanks de EEUU (Contreras; Barrett, 2020), como New American Security y el Council of Foreign Relations, cuyo alineamiento con la política exterior estadounidense es notorio. En todos estos casos, es difícil de encontrar la presencia de la voz de especialistas de América Latina, y menos aún de voces críticas.

En otras palabras, la prioridad que CICTE le asignó a las fuerzas sociales de EEUU y de sus estados aliados les permitió difundir sus preferencias sobre la gobernanza de la ciberseguridad. La reproducción de estas ideas busca influenciar al resto de los actores participantes de los Estados miembro de la OEA, contribuyendo así a reproducir la ciberhegemonía de EEUU en las Américas.

Fomenta los intereses de las empresas de ciberseguridad de EEUU

Los eventos y vínculos que establece el programa de ciberseguridad de la OEA muestran un sesgo a favorecer a las empresas de EEUU, posicionadas como los actores por excelencia para resolver los desafíos de ciberseguridad en las Américas. En línea con la crítica a los organismos internacional de Cox (1983, p. 173), este representa otro caso donde la transferencia de técnicas modernas de ciberseguridad a los países de la región se realiza de forma funcional a los intereses de las empresas de EEUU, que son las sostienen su liderazgo en el ciberespacio.

Esta influencia se puede apreciar, por un lado, a partir de la sobrerrepresentación de las empresas estadounidenses en los eventos de CIC-

TE y en los trabajos que realizaron para este comité sobre ciberseguridad en las Américas. Por ejemplo, en el simposio de ciberseguridad de 2019, aproximadamente el 30% de los expositores fueron empresas de EEUU auspiciantes de CICTE. Como en años anteriores, varias de ellas elaboraron informes para diagnosticar los desafíos que enfrenta la región, tales como Microsoft, Amazon Web Services, Trend Micro y la Fundación Citi (OEA, 2019b; 2020a).

Por el otro lado, esta influencia se puede inferir de una de las principales fuentes de comunicación del programa de ciberseguridad de la OEA: su cuenta de Twitter (@OEA_Cyber). Por este medio, CICTE anuncia los eventos e informes elaborados con los socios del programa al arrobarlos, por ende, es un indicador indirecto de la importancia asignada a sus patrocinadores. En la Tabla 1 se muestran las primeras diez cuentas más mencionadas, excluyendo aquellas de la OEA. Aunque no son las mayores contribuyentes a los fondos específicos de CICTE, la mitad de las cuentas son de empresas de ciberseguridad de EEUU. Esto indica un sesgo, que contribuye a legitimar los productos y servicios de ciberseguridad de estas firmas en los distintos países de América Latina, sobre los de empresas de otros países.

Tabla 1 - Cuentas de Twitter más mencionados en los tweets de la cuenta del programa de ciberseguridad de la OEA (@OEA_Cyber) producidos entre 27/06/2016 y el 13/01/2021

Nombre de la cuenta	# de menciones en @OEA_Cyber	Descripción
INCIBE	213	Centro Nacional de Ciberseguridad del Gobierno de España
awscloud	157	Empresa de EE.UU.
TrendMicro	146	Empresa de EE.UU.
Citi	123	Empresa de EE.UU.
Cisco LA	90	Empresa de EE.UU.
Microsoft	59	Empresa de EE.UU.
CanadaFP	59	Cuenta sobre las actividades de política exterior de Canadá
Ministerio TIC	49	Ministerio de Tecnologías de la Información y de la Comunicación de Colombia
FIU	49	Universidad Internacional de Florida
LondonCyber	43	Departamento de ciberpolíticas del Ministerio de Relaciones Exteriores del Reino Unido

Fuente: elaboración propia en base a datos recopilados de Twitter.

Asimismo, estos datos apuntan a que la OEA adopta de manera implícita un modelo lineal de la innovación en ciberseguridad, donde las capacidades emanan de EEUU, con algunas contribuciones de España, Canadá, el Reino Unido, y más recientemente Estonia. Por el contrario, el resto de los países de las Américas son entendidos mayoritariamente como meros consumidores de estas tecnologías. Efectivamente, en la revisión de documentos del programa es notable la falta de iniciativas que

contribuyan al desarrollo de capacidades autóctonas de investigación e innovación en ciberseguridad. Recién en 2020 la OEA realizó algo al respecto por medio del establecimiento de un fondo de 200.000 US$, en conjunto con la empresa CISCO y la Fundación CITI, para financiar proyectos de innovación en ciberseguridad (OEA, 2020b). No obstante, el monto del fondo sugiere un compromiso insuficiente en cultivar capacidades de ciberseguridad autóctonas en los Estados miembro.

Obstaculiza el cuestionamiento a los ciberataques y al ciberespionaje de EEUU en el ciberespacio

A diferencia de la OTAN, donde las actividades de ciberseguridad son estimuladas por la amenaza rusa, o de la ASEAN, donde el recelo hacia China es fuerte, la amenaza en la agenda de ciberseguridad de la OEA está enfocada en cibercriminales, ciberterroristas, u otros actores Estatales extrarregionales. Sin embargo, dada la influencia material y de ideas de EEUU en la OEA, esta agenda de amenazas omite uno de los mayores retos de ciberseguridad que enfrentan los países de la región: el exceso de capacidades de ciberataques y de ciberespionaje de EEUU.

En efecto, a partir de los atentados del 2001, el Departamento de Defensa de EEUU ha vigorizado su estrategia para ganar ciberguerras por intermedio del desarrollo de sofisticadas capacidades ofensivas, defensivas y de ciberespionaje (Manjikian, 2010; Zittrain, 2017). Estas capacidades son superiores a las de cualquier otro país del mundo. Durante la administración Trump, EEUU publicó su última estrategia de ciberseguridad, donde se delinea la doctrina de combate permanente (permanente engagement) (The White House, 2018), que habilita al cibercomando de EEUU a hackear preventivamente a sus rivales, dondequiera que operen (US Cyber Command, 2018).

Incluso previo a esta estrategia pugnaz, numerosas revelaciones y noticias de seguridad informática expusieron el uso que EEUU le dio a sus capacidades de ciberataques y de ciberespionaje alrededor del planeta. Por ejemplo, Edward Snowden reveló el programa PRISM, que le permitía a la Agencia Nacional de Seguridad (NSA), en colaboración con las principales empresas de Internet estadounidenses, espiar a líderes y ciudadanos de países rivales y aliados por igual, develando un Estado de vigilancia global (Baumann *et al*., 2014). En 2015, investigaciones de la empresa Kaspersky expusieron al grupo de hackers más sofisticado del planeta, Equation Group, cuyas actividades fueron aparentemente realizadas bajo la dirección de la NSA. Igualmente, WikiLeaks hizo público parte del arsenal de ciberarmas de la CIA. En América Latina, estas prácticas afectaron a políticos, empresas y ciudadanos de Argentina, Brasil, Colombia, Ecuador, México, Venezuela, entre otros. Por ende, los ciberataques y el ciberespionaje de EEUU en el ciberespacio ya son una realidad hace años.

El caso Snowden tuvo repercusiones en la OEA. En 2013, el avión del entonces Presidente Evo Morales se vio forzado a detenerse en Austria, tras que España, Francia, Italia y Portugal le negaran el tránsito por su espacio aéreo. La causa fue la presunta presión de EEUU a sus aliados

europeos para corroborar si Snowden viajaba en la aeronave presidencial boliviana. Si bien casi todos los Estados miembros del Consejo Permanente de la OEA emitieron una declaración condenando lo acontecido, EEUU y Canadá se negaron en base a la existencia de 'interpretaciones conflictivas' del hecho (OEA, 2013b).

CONCLUSIONES

El artículo propuso extender el clásico concepto de hegemonía de Cox al ciberespacio como alternativa al concepto de ciberpoder. Esta conceptualización de ciberhegemonía, que entiende a las organizaciones internacionales como mecanismos de una estructura ciberhegemónica mundial, se empleó para argumentar que el programa de ciberseguridad de la OEA reproduce la ciberhegemonía de EEUU en las Américas. De hecho, desde 2004 se constituyó como el principal organismo regional en el tema de la ciberseguridad, donde los diplomáticos, funcionarios y otros actores de los Estados miembro intercambiaron experiencias, conocimientos y formas de entender y actuar en el ciberespacio. En particular, las actividades vinculadas a la ciberseguridad realizadas por CICTE abarcaron el apoyo a la construcción de una red regional de CSIRTs, el asesoramiento a varios gobiernos en la elaboración de sus estrategias nacionales de ciberseguridad, y la capacitación a numerosos actores de la región, entre otras. Estos esfuerzos de construcción de una ciberhegemonía regional se realizaron de forma consensual, en particular, con la aquiescencia de los gobiernos de orientación política más cercana a EEUU.

Sin embargo, el análisis también indica que el programa de ciberseguridad de la OEA provoca efectos adversos para las políticas de ciberseguridad de los países de América Latina. En primer lugar, reproduce y legitima las ideas de las fuerzas sociales de EEUU,y en menor medida, las de sus Estados aliados. El halo de influencia de la superpotencia en el programa se expresa tanto en la definición de la agenda temática, como en la sobrerrepresentación de sus empresas y especialistas de ciberseguridad en sus seminarios, talleres y otros eventos. En segundo lugar, la OEA fomenta los intereses de las empresas de ciberseguridad de EEUU sobre los de empresas de otros países. En efecto, se argumentó que implícitamente adopta un modelo lineal de innovación al propiciar la transferencia de capacidades a los Estados miembros, quienes son vistos como meros consumidores de conocimientos y herramientas elaboradas principalmente por empresas de EEUU. Por último, a pesar de que EEUU tiene las mayores capacidades de ciberataques y de ciberespionaje del mundo, con antecedentes polémicos de su uso a nivel global y en la región, el hecho de que sea el principal financista de la OEA obstaculiza el cuestionamiento a sus ciberataques y a sus actividades de ciberespionaje por parte del resto de los Estados miembro.

REFERENCIAS

ARANDA B. G.; RIQUELME R. J.; SALINAS C. S. La ciberdefensa como parte de la agenda de integración sudamericana. **Línea Sur**, n. 9, p. 100–116, 2015.

ARQUILLA, J.; RONFELDT D. Cyberwar is coming!. **Comparative Strategy**, vol. 12, n. 2, p. 141–65, 1993.

BAUMAN, Z.; BIGO D.; ESTEVES, P.; GUILD, E.; JABRI, V.; LYON, D.; WALKER, R.B.J. After Snowden: Rethinking the impact of surveillance. **International Political Sociology**, vol. 8, n. 2, p. 121–44, 2014.

BID; OEA. ¿Estamos preparados en América Latina y el Caribe? Informe ciberseguridad. 2016. Disponible en: https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamospreparados-en-america-latina-y-el-caribe Acceso el 22 jul 2021.

BETZ D.J.; STEVENS T. Chapter one: Power and cyberspace. **Adelphi Series**, vol. 51, n. 424, p. 35–54, 2011.

CASTRO V., H. J.; MONTEVERDE S., A. Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito. **Revista Espacios**, vol. 39, n. 39, 2018.

CICTE. **Declaración de San Carlos sobre cooperación hemisférica para enfrentar el terrorismo de manera integral**. 2006. Disponible en: http://www.oas.org/es/sms/cicte/documents/sesiones/2006/Sexto_Periodo_Declaracion%20de%20San%20Carlos%20IC00563%20S%20(1).pdf Acceso el 22 jul 2021.

CONTRERAS, B.; BARRETT, K-A. Challenges in building regional capacities in cybersecurity: A regional organizational reflection. In: TIKK, E.; KERTTUNEN, M. **Routledge handbook of international cybersecurity.** Abingdon: Routledge, 2020, Cap 16. p. 214–7.

COX, R. W. Social forces, states and world orders: Beyond international relations theory. **Millennium - Journal of International Studies**, vol. 10, n. 2, p. 126–55, 1981.

COX, R. W. Gramsci, hegemony and international relations : An essay in method. **Millennium: Journal of International Studies**, *vol.* 12, n. 2, p. 162–75, 1983.

DUNN C., M. D. Cyber-terror—Looming threat or phantom menace? The framing of the US cyber-threat debate. **Journal of Information Technology & Politics**, vol. 4, n. 1, p. 19–36, 2008.

DUNN C., M. D. Europe's cyber-power. **European Politics and Society**, vol. 19, n. 3, p. 304–20, 2018.

DUNN C., M. D. Cybersecurity between hypersecuritization and technological routine. In: TIKK, E.; KERTTUNEN, M. **Routledge handbook of international cybersecurity**. Abingdon: Routledge, 2020, Cap 1. p. 11–21.

GARCINUÑO, P. La OEA y el gobierno de Colombia unen fuerzas por la seguridad cibernética. **InnovaSpain**, 27 julio, 2016. Disponible en: https://www.innovaspain.com/la-oea-gobierno-colombia-unen-fuerzas-la-seguridad-cibernetica/ Acceso el 22 jul 2021.

HERZ, M. Does the Organisation of American States matter?. **Crisis States Working Paper Series 2**. London, UK: Crisis States Research Centre, 2018. Disponible en: http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/csrc-working-papers-phase-two/wp34.2-does-the-oas-matter.pdf Acceso el 22 jul 2021.

KACOWICZ, A. M.; PRESS-BARNATHAN, G. Regional Security Governance. In: Tanja A. BÖRZEL, T. A.; RISSE, T. : **The Oxford handbook of comparative regionalism**. Oxford: Oxford University Press, 2016, Cap. 15, p. 297-322.

KAPLAN, F. **Dark territory. The secret history of cyber war**. New York, USA: Simon & Schuster, 2016.

KERTTUNEN, M.; TIKK, E. Introduction. In: TIKK, E.; KERTTUNEN, M. **Routledge Handbook of international cybersecurity.** Abingdon: Routledge, 2020, p. 1–8.

LONG G. How Washington controls its backyard: The Ministry of American Colonies. **Le Monde Diplomatique**, mayo 2020. Disponible en: https://mondediplo.com/2020/05/13oas Acceso el 22 jul 2021.

LÓPEZ L. A. Cuba y la OEA: Cambio y continuidad. **América Latina Hoy**, vol. 52, p. 107–30, 2009.

MANJIKIAN, M. M. E. From global village to virtual battlespace: The colonizing of the Internet and the extension of realpolitik. **International Studies Quarterly**, vol. 54, n. 2, p. 381–401, 2010.

OAS. **Summary of cybersecurity activities implemented by the CICTE Secretariat**. 2017. Disponible en: http://scm.oas.org/doc_public/ENGLISH/HIST_17/CICTE01105E03.doc. Acceso el 22 jul 2021.

OEA. **Octava reunión de consulta de ministros de relaciones exteriores. Secretaría General de la Organización de los Estados Americanos**. 1962. Disponible en: https://www.oas.org/consejo/sp/rc/Actas/Acta%208.pdf. Acceso el 22 jul 2021.

OEA. **Cooperación hemisférica para prevenir, combatir y eliminar el terrorismo**. 1999. Disponible en: http://www.summit-americas.org/OAS%20General%20Assembly/AG-RES-1650-sp.htm Acceso el 22 jul 2021.

OEA. **Declaración de San Salvador sobre el fortalecimiento de la cooperación en la lucha contra el terrorismo**. 2003a. Disponible en: http://www.oas.org/OASpage/Terrorismo/declaracion-sansalvador-esp.htm Acceso el 22 jul 2021.

OEA. **Declaración sobre seguridad en las Américas**. 2003b. Disponible en: http://www.oas.org/36AG/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf Acceso el 22 jul 2021.

OEA. **Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética**. 2004. Disponible en: http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp Acceso el 22 jul 2021.

OEA. **Report of the rapporteur of the seventh regular session of the Inter-American Committee Against Terrorism. Appendix**. 2007. Disponible en: http://www.oas.org/en/sms/cicte/Documents/Sessions/2007/CICTE%20VII_Rapporteur%20Report_CICTE001888E.pdf Acceso el 22 jul 2021.

OEA. **Declaración "Fortalecimiento de la seguridad cibernética en las Américas"**. 2012a. Disponible en: https://www.oas.org/es/sms/cicte/documents/sesiones/2012/DEC%201%20rev%201%20DECLARACION%20CICTE00749S04.pdf Acceso el 22 jul 2021.

OEA. **Remarks by Mr. Christopher Painter, coordinator for cyber issues, Department of State, United States of America: Strengthening cyber security in the Americas**. 2012b. Disponible en: https://www.oas.org/es/sms/cicte/documents/sesiones/2012/CICTE%20INF%204%20REMARKS%20BY%20CHRISTOPHER%20PAINTER%20CICTE00755E04.pdf Acceso el 22 jul 2021.

OEA. **Report on activities of the Secretariat of the Inter-American Committee against Terrorism**. 2013a. Disponible en: https://www.oas.org/en/sms/cicte/Documents/Sessions/2013/REPORT%20ON%20ACTIVITIES%20OF%20CICTE%20CICTE00820S03.pdf Acceso el 22 jul 2021.

OEA. **Solidaridad de los Estados miembros de la OEA con el presidente del Estado plurinacional de Bolivia Evo Morales Ayma y el pueblo boliviano**. 2013b. Disponible en: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=D-012 Acceso el 22 jul 2021.

OEA. **Report on the activities of the Secretary of the Inter-American Committee Against Terrorism**. 2014. Disponible en: https://www.oas.org/es/sms/cicte/documents/sesiones/2014/CICTE%20DOC%204%20REPORT%20ON%20ACTIVITIES%20OF%20THE%20SECRETARIAT%20CICTE00895E04.pdf Acceso el 22 jul 2021.

OEA. **Informe de la presidenta del Comité Interamericano Contra el Terrorismo 2014-2015, Jennifer May Loten, Representante permanente interina de Canadá ante la OEA**. 2015a. Disponible en: https://www.oas.org/es/sms/cicte/documents/sesiones/2015/CICTE%20DOC%204%20COR%201%20INFORME%20DE%20LA%20PRESIDENTA%20DEL%20COMITE%20CICTE00962S04.pdf Acceso el 22 jul 2021.

OEA. **Declaración protección de infraestructura crítica ante las amenazas emergentes**. 2015b. Disponible en: https://www.oas.org/es/sms/cicte/documents/sesiones/2015/CICTE%20DOC%201%20DECLARACION%20CICTE00955S04.pdf Acceso el 22 jul 2021.

OEA. **Fortalecimiento de la cooperación y del desarrollo en la seguridad cibernética y la lucha contra el terrorismo en las Américas**. 2016. Disponible en: http://www.oas.org/en/sms/cicte/Documents/2016/Declaration/CICTE%20DEC%201%20DECLARACION%20ESPANOL%20CICTE01037S04.pdf Acceso el 22 jul 2021.

OEA. **Informe anual 2018 del Comité Interamericano Contra El Terrorismo (CICTE) al cuadragésimo noveno período ordinario de sesiones de la Asamblea General.** 2019b**.** Disponible en: http://scm.oas.org/IDMS/Redirectpage.aspx?class=X.2.19%20CICTE/Doc&classNum=7&lang=s Acceso el 22 jul 2021.

OEA. **Informe anual 2019 del Comité Interamericano Contra el Terrorismo (CICTE) al quincuagésimo período ordinario de sesiones de la Asamblea General**. 2020a. Disponible en: http://scm.oas.org/IDMS/Redirectpage.aspx?class=X.2.20%20CICTE/doc.&classNum=5&lan-

g=s Acceso el 22 jul 2021.

OEA. **OEA, Cisco y la Fundación Citi abren postulaciones para el fondo de innovación de ciberseguridad, dotado con US$200.000**. 2020b. Disponible en: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-108/20 Acceso el 22 jul 2021.

OEA; TREND MICRO. **Reporte de seguridad cibernética e infraestructura crítica de las Américas**. Washington DC, USA, 2015.

OEA; SYMANTEC. **Tendencias de seguridad cibernética en América Latina y el Caribe**. Washington DC, USA, 2014.

PAINTER, C. **Remarks for Christopher Painter. Coordinator for cyber issues, U.S. Department of State**. 2016. Disponible en: http://www.oas.org/en/sms/cicte/Documents/2016/Speeches/2016-02-25%20Remarks%20for%20Christopher%20Painter%20-%20CICTE%20National%20Points%20of%20Contact%20Meeting_FINAL.pdf Acceso el 22 jul 2021.

RID, T. Cyber war will not take place. **The Journal of Strategic Studies**, vol. 35, n. 1, p. 5-32, 2012.

SANCHO H., C. Ciberseguridad. Presentación del dossier. **Revista Latinoamericana de Estudios de Seguridad**, n. 20, p. 8–15, 2017.

STONE, J. Cyber war will take place!. **Journal of Strategic Studies**, vol. 36, n. 1, p. 101–8, 2013.

THE WHITE HOUSE. **The national strategy to secure cyberspace**. 2003. Disponible en: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf Acceso el 22 jul 2021.

THE WHITE HOUSE. **International strategy for cyberspace: Prosperity, security, and openness in a networked world**. 2011. Disponible en: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf Acceso el 22 jul 2021.

THE WHITE HOUSE. **National cyber strategy of the United States of America**. 2018. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf Acceso el 22 jul 2021.

THÉRIEN, J-P.; GORDON M.; GAGNÉ S. The changing dynamics of Inter-American security. **Latin American Policy**, vol. 3, n. 2, p. 147–63, 2012.

US CYBER COMMAND. **Achieve and maintain cyberspace superiority: Command vision for US Cyber Command**. Abril 2018. Disponible en: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf Acceso el 22 jul 2021.

VALERIANO, B.; MANESS, R.C. The dynamics of cyber conflict between rival antagonists, 2001-11. **Journal of Peace Research**, vol. 51, n. 3, p. 347–60, 2014.

VILA SEOANE, M.; SAGUIER, M. Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional, **Relaciones Internacionales**, n. 40, p. 113-131, 2019.

WEIFFEN, B. Persistence and change in regional security institutions: Does the OAS still have a project?. **Contemporary Security Policy**, vol. 33, n. 2, p. 360–83, 2012.

WEIFFEN, B.; WEHNER L.; NOLTE D. Overlapping regional security institutions in South America: The case of OAS and UNASUR. **International Area Studies Review**, vol. 16, n. 4, p. 370–89, 2013.

ZITTRAIN, J. 'Netwar': The unwelcome militarization of the Internet has arrived. **Bulletin of the Atomic Scientists**, v. 73, n. 5, p. 300–304, 2017.