El sistema internacional cibernético: elementos de análisis

Germán Alejandro Patiño Orozco*

RESUMEN

Este artículo aporta algunas consideraciones sobre el debate de cuestiones cibernéticas y sus efectos sobre el entendimiento de nuevas temáticas de seguridad internacional. Además, propone la adopción de metodologías de la disciplina de relaciones internacionales para estudiar asuntos cibernéticos de carácter global. El artículo concluye con algunos lineamientos para profundizar acerca del análisis de temas cibernéticos con una perspectiva internacional.

Palabras clave: ciberseguridad, ciberespacio, seguridad internacional, sistema internacional cibernético.

The international cybersystem: elements of analysis

ABSTRACT

This article provides insights into the debate about cyber issues and its effects on our understanding of new international security topics. Moreover, this article proposes the adoption of principles from the discipline of International Relations to study cyber issues in the global realm. The article concludes by offering certain guidelines to delve further in the analysis of cyber topics from an international perspective.

Key words: cyberspace, cybersecurity, international security, international cybersystem.

---

* Maestría en estudios de Asia y África con especialidad en China por el Centro de Estudios de Asia y África de El Colegio de México. Candidato a doctor en estudios de desarrollo global por la Universidad Autónoma de Baja California. Universidad Autónoma de Baja California (UABC). Profesor de la Facultad de Economía y Relaciones Internacionales en la Universidad Autónoma de Baja California. Tijuana, Baja California, (México). [german.patino@gmail.com]; [https://orcid.org/0000-0003-0275-0238].

Recibido: 29 de marzo de 2019 / Modificado: 10 de mayo de 2019 / Aceptado: 14 de mayo de 2019

Para citar este artículo:

Patiño Orozco, G.A. (2019). El sistema internacional cibernético: elementos de análisis. *OASIS*, 30, pp. 163-186.

DOI: https://doi.org/10.18601/16577558.n30.10

INTRODUCCIÓN

Entre la primera y la segunda década del siglo xxi, hasta cierto punto, las cuestiones relacionadas con el ciberespacio y sus usos han construido una narrativa que los considera la quintaesencia del marco de análisis de la seguridad internacional. Ahora se aprecia que las cualidades del ciberespacio son tanto una fuente de desarrollo y progreso como de vulnerabilidad, así como una herramienta de control y de ataque, que representan una amenaza potencial para la *seguridad* y una perturbación del orden internacional conocido (Choucri, 2012, p. 3). Desde ese punto de vista, el ciberespacio es la principal zona de disputa en política internacional. Allí se puede observar que el enfoque dominante es el desarrollo de un proceso de construcción de la amenaza cimentado en el miedo (Valeriano & Maness, 2015; Klimburg, 2017) (Dunn Cavelty, 2008b). Para algunos, ese miedo está asociado fuertemente con las acciones del 11 de septiembre de 2001, pero se ha disipado y, en cierta forma, ha sido reemplazado con "el miedo de un posible conflicto cibernético, e incluso de una guerra cibernética" (Valeriano & Maness, 2015, p. 2).

Con base en lo anterior, el interés de la presente investigación es analizar la literatura que ha abordado la interrelación entre la seguridad internacional y el ciberespacio. En este trabajo se reconoce que la seguridad cibernética, llamada *ciberseguridad*, es un área que involucra la participación de múltiples actores sociales y políticos, no obstante, se pretende analizar, en particular, el entendimiento que ha tenido el Estado en el ciberespacio y sus efectos sobre el funcionamiento de este.

En relación con lo antes expuesto, dentro de este artículo se busca dar respuesta al siguiente interrogante que funciona como guía a lo largo de la investigación, ¿cómo se ha estudiado la participación estatal en el espacio cibernético?, ¿cómo ha evolucionado el abordaje teórico de la seguridad internacional en relación con las actividades cibernéticas? Como tesis central de este trabajo se propone que la magnitud, el alcance y la variedad de las actividades cibernéticas es tan extensa que conduce a la restructuración teórica en aras de estar capacitados para enfrentar un fenómeno contingente, multidimensional y multidisciplinar.

Con base en esto, la amplia gama de percepciones que los principales actores internacionales tengan puede causar una profunda transformación en la estructuración del entorno internacional, así como también sobre la normatividad internacional, en este caso en el entendimiento de una concepción fija sobre la ciberseguridad y su asociación con un entorno cibernético internacional determinado. Por tanto, el reto es examinar las raíces del cambio y sus interconexiones.

Este artículo está organizado en cuatro rubros. En primer lugar, revisa el tratamiento que se ha dado a las cuestiones tecnológicas, en particular del entorno cibernético en la disciplina de relaciones internacionales. En segundo lugar, rastrea el origen conceptual de lo cibernético y su conformación como un esquema de interacción, así como la incipiente configuración de un sistema internacional cibernético y sus principales características. En la tercera sección se realiza la propuesta sobre la conformación de este y las particularidades que le dan forma y lo hacen diferente al sistema in-

ternacional cinético. Por último, se identifican los vacíos epistemológicos de la temática desde la perspectiva de relaciones internacionales y se realiza una exhortación hacia un abordaje sistemático y holístico sobre este fenómeno internacional incipiente.

I. EL DEBATE SOBRE LA SEGURIDAD CIBERNÉTICA INTERNACIONAL

Cualquier tecnología puede ser estudiada desde una variedad de perspectivas: *1)* por medio de las costumbres que origina; *2)* las relaciones sociales que ayuda a fomentar; *3)* el desarrollo de ciertas prácticas; y *4)* los valores que fomenta. Asimismo, estudiar la tecnología en contextos culturales permite entender en qué medida la especie humana está condicionada por la estructura sistémica en la que se desenvuelve y cómo, a su vez, esta (la agencia) influye en la estructura mediante su interacción social en función de la multiplicidad de intereses determinados por enlaces crecientes de intereses e identidades colectivas (Escobar, 1994).

La reestructuración de relaciones con base en la tecnología funciona como un agente de producción social y cultural (Escobar, 1994). El origen y la operación de estos enlaces permiten observar la continuidad y la transformación de los valores dominantes de racionalidad, instrumentalidad, ganancia y violencia que están circunscritos, regularmente, por intereses económicos y político-militares (Escobar, 1994). Los avances en la tecnología, respaldados por la innovación científica, han permitido el acceso a nuevas formas de espacio. La innovación tecnológica también ha mejorado nuestra capacidad de delinear el conocimiento sobre las propiedades y características de ámbitos de actividad en otros territorios previamente inaccesibles. No obstante, estas tecnologías pueden también ser objeto de abuso para producir condiciones desestabilizadoras, como el desarrollo de armas de destrucción en masa, instrumentos de dominación, control y explotación, sobre todo a medida que se vuelven más económicas y la capacidad de obtenerlas y manipularlas se generaliza (Choucri, 2012, p. 6).

Dentro de este cuadro se puede enmarcar el estudio del espacio digital. Creado a través de la innovación tecnológica permite a los usuarios participar en actividades dentro de campos electrónicos cuyos dominios espaciales trascienden las restricciones territoriales, gubernamentales, sociales y económicas tradicionales (Mattelart, 2007; Choucri, 2012, p. 6). Este espacio ofrece nuevas oportunidades para la competencia, la colaboración, la contención, el conflicto y la cooperación.

De ordinario, los nuevos espacios se han formado mediante el despliegue de la fuerza física combinada con el poder de la competencia, la innovación y el espíritu de aventura. Históricamente, solo los actores más capaces, los más poderosos y eficaces, militarmente o no, han podido competir en efecto, en la colonización del territorio y la exploración de los espacios (Krishna-Hensel, 2007). Estos espacios se han entendido claramente como el lugar donde está la búsqueda del poder, el prestigio colectivo, el posicionamiento en el panorama internacional, la mejora de la riqueza y la ventaja estratégica en la competencia militar, y se llevaron a cabo a través de la expansión física en los territorios (Choucri, 2012, p. 6).

Las interacciones internacionales de todo tipo están cambiando debido a la llegada de las tecnologías cibernéticas. El espacio digital es ahora un lugar de competencia entre intereses y grupos de interés diversos, así como también una arena para conflictos y colaboración que marcan la pauta de los reacomodos sociales, económicos, políticos, culturales e identitarios (Choucri, 2012). Sin embargo, la interrelación entre relaciones internacionales e interacciones cibernéticas, se ha abordado escasamente (Eriksson & Giacomello, 2007).

En particular, la seguridad cibernética ha sido un problema relativamente ignorado por la academia, en especial la comunidad epistémica de las relaciones internacionales. Llama la atención, en especial, la ausencia de bibliografía que se produce en el área de relaciones internacionales. Existen pocos análisis sistemáticos, teóricos o empíricos del problema cibernético desde la disciplina de las relaciones internacionales o desde el subcampo de los estudios de seguridad (Deibert, 2003; Eriksson & Giacomello, 2006; Hansen & Nissenbaum, 2009; Valeriano & Maness, 2015; McEvoy, 2010; Klimburg, 2017; Eriksson & Giacomello, 2007; Rid, 2012; Arquilla & Ronfeldt, 1993). No obstante, destaca la aportación seminal que hicieron John Arquilla y David Ronfeldt (1993) sobre la emergencia de nuevos modos de conflicto, el desarrollo de conceptos como "ciberguerra" o "guerra en red" (*netwar*) y el impacto de las tecnologías de la información digital sobre el conflicto internacional. Por otra parte, autores como Thomas Rid (2012) cuestiona que la guerra cibernética y los desarrollos digitales tengan un impacto significativo sobre los asuntos polemológicos.

Existe cierto consenso entre los autores acerca de la causa principal que supuestamente explica la situación de escasez analítica del tema. Para algunos autores, esto responde a un importante grado de escepticismo sobre la relevancia del ecosistema cibernético de carácter internacional como un importante componente para explicar el cambio y la transformación a nivel internacional, por ende, la escasa literatura de relevancia (Choucri, 2012; Kello, 2013; Valeriano & Maness, 2015). Para otros autores, el desarrollo poco profuso desde la perspectiva de relaciones internacionales se debe a una 'obsesión' al interior de la disciplina por brindar esquemas teóricos generales con poca aplicabilidad empírica, dejando de lado cuestiones como el desarrollo tecnológico y su impacto sobre el esquema político, económico y social de carácter global (Eriksson & Giacomello, 2007, p. 2).

Existe una dicotomía en relación con los supuestos sobre la correspondencia entre el dominio digital y la política. Algunos consideran que esta arena modifica, en absoluto, todas las actividades humanas formando nuevos ecosistemas, por medio de mayor información asequible y un grado superlativo de transparencia política (Castells, 2009; Zittrain, 2008). En ese tenor, algunos recalcan que las herramientas de interacción social digital coadyuvan en la construcción de la esfera pública internacional (Shirky, 2011). No obstante, esta visión desestima los efectos negativos de la red. Por su parte, otros consideran que el espacio digital modifica pocas situaciones, puesto que gobiernos y agentes privados continúan utilizando su fuerza militar y su influencia económica para asegurar el control y dominio

sobre amplios sectores sociales (Deibert, 2013; Escobar, 1994).

En realidad, suceden ambas tendencias simultáneamente (Wu, 2008, p. 5) (Morozov E., 2011). El desafío es entender cómo las viejas fuentes del poder interactúan con nuevos formatos (Morozov E., 2011). Unos argumentan que el debate de las relaciones cibernéticas necesita moverse hacia las bases del estudio de la política internacional (Choucri, 2012; Kello, 2013; Valeriano & Maness, 2015; Lindsay, 2015a; Eriksson & Giacomello, 2007). En efecto, los problemas cibernéticos internacionales no están desmarcados completamente de los procesos de las relaciones internacionales cinéticos, en otras palabras, "las operaciones que ocurren en el dominio cibernético no están desconectadas de otros dominios de la interacción política internacional" (Valeriano & Maness, 2015, p. 14). Como recalca Brandon Valeriano y Ryan C. Maness (2015, p. 15) "es cierto que el ciberespacio es un dominio con dinámicas propias, pero no está desvinculado totalmente del plano político internacional que es la génesis de los conflictos internacionales".

Antes de continuar con la revisión de los debates teóricos sobre el tema, algunas aclaraciones conceptuales y metodológicas son necesarias para solventar la capacidad explicativa del estudio. Para realizar el análisis propuesto, se debe describir y explicar en qué consiste el espacio en el cual participan los agentes estudiados, la diversidad de su índole, así como su evolución y la diversificación que permite la reconfiguración de fuerzas y actores. En este proceso se articulan prácticas y políticas distintivas y específicas que ayudan a entender la dimensión y el alcance desplegado por las prácticas estatales de seguridad en el terreno cibernético.

A. Antecedentes del sistema internacional cibernético

Las raíces históricas y filosóficas del vocablo "cibernético", a menudo, se considera que aparecieron por primera vez en la obra *La República* del filósofo griego Platón (Klimburg, 2017). Para otros, su identidad semántica para la "edad moderna" se deriva del término *cibernética*, "el estudio de la comunicación y el control" presentado por el matemático Norbert Wiener (1948) en *Cybernetics: Or Control and Communication in the Animal and the Machine* (Escobar, 1994, p. 211; Choucri, 2012, p. 7; Valeriano & Maness, 2015, p. 3; Deibert, 2013)[1].

En consecuencia, el trabajo de Norbert Weiner influyó el de Karl W. Deutsch (1963) *The Nerves of Government*, que sigue siendo un punto de entrada importante en la ciencia política y en la investigación sobre la interrelación entre comunicación, política y control[2]. Por

[1] Cuando Norbert Wiener acuñó el término "cibernética" tenía en mente la labor que los jinetes o los "pilotos" de la Grecia antigua realizaban (*kibernetes*), aunque no exista una raíz etimológica griega para dicha expresión, su uso se ha vuelto un prefijo común para identificar las acciones relacionadas con el espacio digital (Escobar, 1994).

[2] Karl Deutsch utilizó elementos de la teoría de las comunicaciones y cibernética, así como de la sociología estructural-funcionalista. La sociología estructural-funcionalista estudia la sociedad como una totalidad formada por partes interdependientes, cada una de las cuales cumple una función en el mantenimiento y la reproducción del sistema. El concepto

otra parte, el autor de ciencia ficción William Gibson (1984) es reconocido por ser el primero en acuñar el vocablo *ciberespacio* en su obra *Neuromancer*[3], proporcionando la primera designación formal que integraba las nociones de cibernética y espacio, y así dar cabida a la creación de un nuevo campo de interacción (Choucri, 2012, p. 7). Por otro lado, el sitio tecnológico *Gizmodo* rastreó la vida del prefijo '*ciber*' desde 1950 hasta 2013, y encontró las variaciones que el concepto cibernético ha tenido (Klimburg, 2017, p. 23).

En torno a ello, han surgido diversas definiciones y concepciones de lo que el *ciberespacio* representa y los elementos que lo componen. Por ejemplo, para autores como Richard Clarke y Robert K. Knake (2010, p. 70) lo definen como "todas las redes de computadora en el mundo y todo con lo que conectan y controlan". No obstante, limitar lo cibernético (*cyber*) a redes computacionales es un poco estrecho y restringe la integración de nuevas tecnologías cibernéticas dentro del paradigma. Para otros autores, la inclusión del término *microprocesador* puede proveer de mayor precisión a una definición del ciberespacio (Valeriano & Maness, 2015, p. 22). Por su parte la definición que propone Joseph Nye (2011) está mucho más cerca del contenido real de lo que es el ciberespacio para la mayoría de quienes utilizan el término en el contexto político. Para Nye (2011), "el dominio cibernético incluye la red de computadoras conectadas a internet, pero también incluye las redes internas (*intranet*), las tecnologías de telefonía móvil, cables de fibra óptica, comunicación satelital-espacial. Asimismo, el ciberespacio tiene una capa de infraestructura física que está sujeta a leyes económicas, leyes políticas de soberanía, competencia por recursos y por justificar su control y regulación" (Nye, 2011, p. 19).

Para los propósitos de este trabajo de investigación, se tomará al prefijo "*cibernético*" (*cyber*) simplemente con el sentido de las interacciones digitales, computarizadas, o realizadas a través de microprocesadores, las cuales están directamente relacionadas con el ciberespacio y permiten la comunicación e interacción de diversos agentes. Aunque ciberespacio e internet se han utilizado de manera intercambiable, no son lo mismo. Internet es la red global de redes de computadoras configuradas para operar de acuerdo con un protocolo de intercomunicación (*TCP/IP protocol*). El ciberespacio es mucho más amplio e incluye el dominio entero de las comunicaciones globales, donde se incluye (pero no se limita) al internet (Deibert, 2013; Klimburg, 2017).

Aunque la palabra ciberespacio ha tomado diferentes significados derivados de sus características fundamentales, aquí se utiliza la relacionada con la red y que está sostenida por la computación, que permiten el acceso a través de una computadora a la realidad artificial, virtual o digital multidimensional (Benedikt, 1994, p. 122). Para el ámbito que compone

de sistema, entendido como una red de comunicaciones análoga al sistema nervioso es central en su obra (Choucri, 2012; Santa Cruz, 2000, pp. 50-51).

[3] Para algunos autores, el nacimiento del término se da en la pequeña historia intitulada "Burning Chrome" y que fue popularizada en su novela *Neuromancer* (Deibert, 2013, p. 264).

el *ciberespacio* (*cyberspace*), en este trabajo de investigación se toma la siguiente definición: "el sistema en red de microprocesadores, servidores, y computadoras que interactúan en el nivel digital" (Deibert, 2013; Mattelart, 2007; Valeriano & Maness, 2015).

De suma importancia para este trabajo son las formas en que los espacios cibernéticos se utilizan para dar forma a las ideas, intercambiar información y aumentar el acceso al conocimiento y modos alternativos de razonamiento. En efecto, como lo dice el artículo de John Palfrey (2010), todas estas visiones describen una forma de la relación entre el uso de la tecnología y los impactos en la actividad social, que van de la mano con su clasificación de las etapas de desarrollo del ciberespacio.

De igual manera, en relación con la introducción del término *ciberseguridad* o seguridad cibernética no existe un contexto tan amplio. De acuerdo con algunos analistas, el concepto fue utilizado por primera vez en 1989 (Newitz, 2013). Para otros especialistas, el asentamiento de la idea de *ciberseguridad* en el terreno político surge en 1995, cuando la revista *Time* publicó en la portada principal el término '*ciberguerra*' (Klimburg, 2017, p. 23). Quizá esta sea una de las raíces de la asociación de la narrativa de lo cibernético con el miedo.

A este respecto, para 1999, un oficial de alto rango del Departamento de Defensa de los Estados Unidos utilizó el concepto '*ciberguerra*' por primera vez ante el Congreso de su país, marcando un enlace entre el conflicto internacional y las herramientas de explotación computacional como el *hackeo* (Klimburg, 2017, p. 24). No obstante, para una comprensión más clara, se necesita trazar, de forma sistémica, una cronología sobre el desarrollo de lo cibernético de carácter internacional, estableciendo un terreno empírico y teórico que sirva para comprender las relaciones internacionales de cooperación y conflicto que surgen en una dimensión emergente, donde las posturas y visiones son tan diversas como el número de actores.

B. Fases del sistema internacional cibernético

De acuerdo con algunos especialistas, la interrelación entre el desarrollo cibernético y la seguridad internacional, se puede identificar, bajo las siguientes fases del desarrollo del ciberespacio: *1)* la era abierta, que va desde su nacimiento hasta el 2000; *2)* el acceso denegado, de 2000 a 2005; *3)* el acceso controlado, de 2005 a 2010 y; *4)* acceso en disputa, de 2010 a la actualidad (Palfrey, 2010, p. 981). De acuerdo con John Palfrey (2010), la primera etapa corresponde a la arquitectura y los cimientos de la red global, donde el propósito central de su desarrollo era que fungiera como una herramienta para el intercambio de comunicación de forma libre, utilizada por algunas instituciones académicas y gubernamentales de Estados Unidos. Este funcionamiento comienza a ceder paso a finales de la década de 1980, cuando nace la *World Wide Web*, y comienza lo que algunos autores denominan "la comercialización de internet" (Perrit, 1998; Sassen, 1998).

En la segunda etapa, ciertos actores estatales y no estatales consideraban que algunas actividades que comenzaban a desarrollarse en internet necesitaban ser reguladas o interceptadas, principalmente algunas muestras de libertad de expresión, creando fuertes filtros para el acceso a

la información (Palfrey, 2010, p. 985; Morozov E., 2011). Dentro de una concepción general, se considera que únicamente algunos gobiernos (calificados como autoritarios o no democráticos) son propensos a utilizar filtros para bloquear el contenido que fluye dentro de sus fronteras a través del ciberespacio, sin embargo, es una actividad realizada también por gobiernos democráticos, en ocasiones apoyados por empresas privadas que manejan una gran cantidad de los flujos informativos en la red (Deibert, Palfrrey, Rohozinski & Zittrain, 2008; Deibert & Rohozinsky, 2010; Vaidhyanathan, 2018).

Estos controles demuestran lo que algunos han tratado de enfatizar sobre en qué medida la teoría tradicional de las relaciones internacionales gobierna tanto en el espacio real como en el ciberespacio (Goldsmith & Wu, 2006; Palfrey, 2010). Precisamente, la tercera fase se caracteriza como un período durante el cual los Estados han enfatizado sobre enfoques regulatorios que sirven como variables de control (Palfrey, 2010, p. 989). Lo destacado de este tiempo es el desarrollo de la noción de que existen una serie de mecanismos que pueden utilizarse para limitar el acceso a la información, que son más sofisticados y rebuscados que en la etapa anterior (Deibert, Palfrey, Rohozins & Zittrain, 2010; Morozov E., 2011). Dentro de esta etapa surgen requerimientos como el registro de usuarios, licencias de uso y controles legales sobre la forma de utilizar el ciberespacio. A su vez, se observa una combinación entre vigilancia y medios de imposición, aplicación y ejecución legal, que para algunos tiene un efecto negativo sobre la libertad de expresión en línea (Morozov E., 2011; Deibert & Rohozinsky, 2010).

Mientras que en la cuarta etapa, la regulación que se ha impuesto comienza a enfrentar respuestas de los ciudadanos y desafíos del sector privado (Deibert, Palfrey, Rohozinski & Zittrain, 2012). Las compañías de tecnología de la información han comenzado a competir directamente, o indirectamente, entre ellas y contra los gobiernos sobre cómo desempeñar el control e incluso la censura, en el ciberespacio (Palfrey, 2010, p. 992; Vaidhyanathan, 2018). Asimismo, los agentes estatales y los organismos internacionales intergubernamentales se han comenzado a enfrascar en fuertes debates y en acciones que buscan regular el ciberespacio en formas divergentes, lo que ha resultado en una disputa sobre la forma de gobernanza del ciberespacio (DeNardis, 2009; 2014).

Estas etapas cronológicas que John Palfrey (2010) encuadra conforme su característica primordial de interrelación entre actores y contexto tratan de describir la utilización, el papel y las prácticas que diversos actores han tenido en el desarrollo del dominio digital, incluidos los agentes estatales. No obstante que su temporalización es muy útil, pareciera que el comienzo de una etapa no rechaza por completo la existencia de la otra, por lo cual se puede afirmar que siguen coexistiendo y retroalimentándose entre sí.

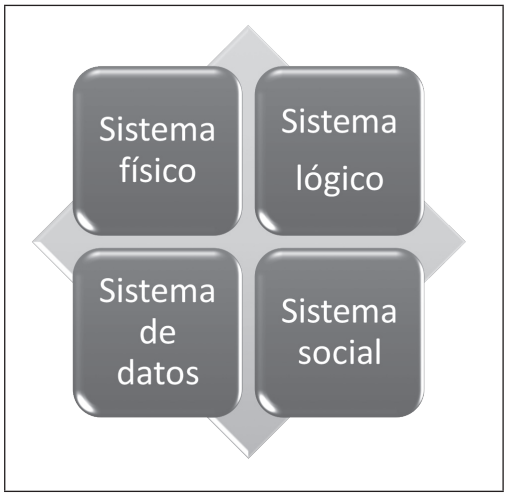
C. Características del sistema internacional cibernético

Ciertamente el ciberespacio es un elemento que genera una reconfiguración de las relaciones internacionales contemporáneas, pero, ¿cuáles son las características de un posible sistema internacional cibernético?, ¿qué componentes

lo forman que lo hacen distintivo del sistema internacional cinético o tradicional? Primeramente, se puede observar el ciberespacio como un sistema contingente compuesto por cuatro categorías: *1)* el primer escalón lo componen los fundamentos físicos e infraestructuras que permiten su funcionamiento; que son los cables de fibra óptica, comunicación satelital, dispositivos digitales, servidores, computadoras, el esqueleto del ciberespacio; *2)* el segundo son los bloques de construcción lógica que soportan la plataforma física y que habilitan los servicios, que son una amalgama de códigos, protocolos, *software* y actualizaciones de estos, que forman las neuronas y se desempeñan como el sistema nervioso del ciberespacio; *3)* la tercer capa es el contenido de información almacenado, transmitido o transformado, y reconfigurado, que incluye documentos, vídeos, imágenes, sonido y mensajes, análogos a los músculos del cuerpo ciberespacial; *4)* y, en última instancia, se encuentran los actores, entidades y usuarios que emiten y ayudan a movilizar la tercera capa, que cuentan con diversos intereses y participan en este campo con distintos papeles, que representan el corazón del sistema (Choucri, 2012, p. 8; Klimburg, 2017, pp. 28-29).

En la siguiente figura se puede observar, de forma esquemática, cómo se configuran los distintos sistemas que componen el ciberespacio. Se elige esta figura, pues se considera que la complementariedad y retroalimentación entre los cuatro bloques es indispensable para el buen desempeño de este. Si bien es cierto que en este trabajo de investigación el énfasis se pone en los últimos dos bloques, no se pierde de vista la aportación y el ejercicio que ejercen los primeros dos, pues son imprescindibles para entender la complejidad de las interacciones cibernéticas internacionales.

Figura 1
Sistemas que componen el ciberespacio



Fuente: Elaboración propia con datos de (Choucri, 2012; Klimburg, 2017).

Además, el ciberespacio se puede definir bajo cuatro principios: *1)* que es replicable, significa que el concepto es expandible y resiliente al mismo tiempo; *2)* consiste en acciones reconocidas, como el escribir mensajes en códigos lingüísticos conocidos en oposición al código binario que la gran mayoría poblacional no entiende (dentro del sistema lógico); *3)* tiende a tener reglas o tecnologías persistentes y, por último; *4)* está dividido entre el estrato físico y el estrato sintético (la información y el conocimiento) (Valeriano & Maness, 2015, p. 24).

Todas estas capas, funciones y entidades son relevantes para las relaciones internacionales en su manifestación cibernética. Como

una amalgama de redes interoperables, se ha convertido en una parte fundamental de la emergente infraestructura de comunicación e interacción global, donde la capa de contenido de información se está expandiendo a tasas exponenciales, generando y transmitiendo nueva información, y a su vez creando más mecanismos para facilitar el uso y la reutilización de contenido (Choucri, 2012, p. 8).

II. LA ORGANIZACIÓN DEL SISTEMA INTERNACIONAL CIBERNÉTICO

De acuerdo con lo antes mencionado, las interacciones internacionales están cambiando debido a la llegada de las tecnologías cibernéticas, pues el ciberespacio es ahora un lugar de competencia entre intereses y grupos de interés, así como también arena para conflictos y colaboración que marcan la pauta de los reacomodos sociales, económicos, políticos, culturales e identitarios (Choucri, 2012). No obstante, el sistema cibernético cuenta con cualidades distintivas cuyas características difieren de las interacciones del sistema social o el sistema ambiental.

Para algunos autores como David D. Clark (2010) la cualidad distintiva reside en que los sistemas de decisión del ciberespacio están involucrando una tremenda gama de actores y entidades en la operación de este. En el nivel más general, incluye a los agentes de la industria de internet e informática, aquellos involucrados en aplicaciones y desarrollo de *software*, proveedores de contenido, gobiernos, organizaciones internacionales, gerentes de espacios en la red, organizaciones no gubernamentales y, lo más importante, una gran amalgama de grupos e individuos a lo largo del orbe. En el siguiente cuadro, se pueden ejemplificar, de manera sencilla, algunas de las diferencias entre el sistema internacional tradicional y el cibernético.

Tabla 1.1
Sistema internacional cibernético

Sistema	Sistema Internacional	Sistema Internacional Cibernético
Actores	– Estados-nación – Organismos internacionales intergubernamentales – Organizaciones no gubernamentales – Agencias regionales – Actores de la sociedad civil organizada	– ICANN (Corporación de Internet para la Asignación de Números y Nombres, Internet Corporation for Assigned Names and Numbers) – Grupo de Trabajo sobre la Gobernanza de internet de las Naciones Unidas (Internet UN Working Group on Internet Governance) – Cumbre Mundial de las Naciones Unidas sobre la Sociedad de la Información (UN World Summit on the Information Society) – Estados-nación

Arena/Contexto	Cinético	Cibernético
Dinámicas/Interacciones	Rígidas, cambian de forma lenta, diversas	Flexibles, cambian de forma vertiginosa, diversas
Gobernabilidad	Estratificada, regularmente la toma de decisiones se da en forma vertical	Flexible, irregularmente estratificada, combina formas verticales y horizontales de toma de decisión

Fuente: Elaboración propia con datos de Valeriano & Maness (2015) y Choucri (2012).

Con base en esto, se puede inferir que en el ciberespacio los actores son diversos, con diferentes grados de poder y capacidades, organización e infraestructura, lo cual hace al análisis mayormente desafiante. Esto acentúa más la necesidad de mover el debate de las relaciones cibernéticas hacia las bases del estudio de la política internacional (Valeriano & Maness, 2015). Para algunos expertos, los problemas cibernéticos internacionales no están desprovistos de los procesos de las relaciones internacionales cinéticas, por ello pueden brindar claves para su estudio sistemático, holístico y heurístico (Dunn Cavelty, 2008b). En el siguiente cuadro se presenta una propuesta de análisis para entender la conformación del Sistema Internacional Cibernético.

Tabla. 1.2
Elementos del Sistema Internacional Cibernético

Elementos	Sistema Internacional Cinético (tradicional)	Sistema Internacional Cibernético
Temporalidad	Proceso de media duración	Instantáneo/quasi-instantáneo
Espacialidad	Sujeto a soberanías territoriales	Trasciende limitaciones geográficas
Extensión	Rigidez entre jurisdicciones	Movilidad entre jurisdicciones
Participación	Altas barreras para la participación política directa	Menores barreras para el activismo y la participación política
Atribución	Se busca la visibilidad en la autoridad de las acciones	Se busca mantener oculta la identidad de las acciones
Rendición de cuentas	Mecanismos tradicionales	Elude mecanismos de responsabilidad tradicional

Fuente: Elaboración propia con datos de Choucri (2012).

III. EL SISTEMA INTERNACIONAL CIBERNÉTICO BAJO LA TEORÍA DE RELACIONES INTERNACIONALES

Aunque el objetivo de este artículo no es brindar un marco teórico genérico para el estudio de las interacciones cibernéticas internacionales, aquí se presentan algunas consideraciones elementales de la teoría de las relaciones internacionales que pueden servir de puente y de hilo conductor para comprender de qué forma la metodología y construcción conceptual de la disciplina de relaciones internacionales puede ayudar a perfilar, de manera más precisa, el fenómeno cibernético.

Por un lado, el realismo es un enfoque dentro de las relaciones internacionales que ha tenido fuerza explicativa y una alta atracción dentro de la comunidad académica durante un largo período de tiempo, principalmente durante la guerra fría. Sus supuestos básicos son: *1)* el Estado es la unidad primaria de análisis; *2)* el Estado actúa de forma racional para satisfacer sus intereses nacionales; *3)* el poder y la seguridad son los valores centrales del Estado (Waltz, 1979; Morgenthau, 1948). En todas las vertientes del realismo, su cosmovisión sobre las interacciones internacionales es esencialmente pesimista (Sterling-Folker, 2013). En otras palabras, para el enfoque realista de relaciones internacionales la anarquía (ausencia de un gobierno central) caracteriza el sistema internacional, lo cual fuerza a los actores a comportarse en función de su interés que es la supervivencia (Waltz, 1979). Para los realistas, las causas del conflicto surgen de la competencia entre Estados que buscan sobrevivir a través de incrementar su seguridad. Por ende, las condiciones anárquicas conducen a un "dilema de seguridad", un proceso en el cual una acción está correspondida con una reacción (Jervis, 1979; Glaser, 2004). Como consecuencia, el poder es medido principalmente en términos de capacidades militares y asociado con la búsqueda de seguridad (Morgenthau, 1948; Gilpin R., 1986).

La emergencia de eventos relacionados con la ciberseguridad presenta una oportunidad para el resurgimiento de la perspectiva realista de relaciones internacionales como herramienta útil para analizar cuestiones como: la competencia de seguridad en el ámbito digital; las estrategias cibernéticas de defensa y ataque y su posible escalamiento a conflictos cinéticos de gran envergadura; el establecimiento de leyes nacionales férreas de vigilancia y control en el ciberespacio; la competencia por el desarrollo de arsenales digitales por actores estatales y no estatales; la apropiación espacial en el terreno digital e, incluso, del uso e implementación de la disuasión en el ciberespacio (Craig & Valeriano, 2018; Edde, 2018; Crosset & Dupont, 2018; Ebert & Maurer, 2014; Reardon & Nazli, 2012; Friis & Ringsmose).

Por consiguiente, conforme lo mencionan algunos teóricos, los enfoques realistas no ven la necesidad de corregir o actualizar sus supuestos teóricos para entender el significado de la seguridad en la era digital, sino adaptar los marcos explicativos existentes a las nuevas realidades prácticas. El Estado sigue siendo visto como el actor más importante, y la definición de seguridad se sigue manteniendo estática, la cual niega que los actores no estatales pueden ejercer algún grado de poder militar (Eriksson & Giacomello, 2006, p. 229).

Por otro lado, el enfoque liberal es una perspectiva muy amplia en cuanto las temáticas que aborda, en la cual se incluyen, entre otros, el idealismo wilsoniano y la teoría neoliberal (Moravcsik, A., 1998; Moravcsik, 1999; Walker, 1993); la teoría de la paz democrática (Russett & Antholis, 1993); la teoría de la interdependencia compleja (Keohane & Nye, 1977), o enfoques sobre la ejecución de políticas domésticas y el papel de instituciones internacionales, la institucionalización y la construcción de regímenes internacionales (Allison & Zelikow, 1999; Risse-Kappen, T., 1995; Snyder, 1991). Los principales supuestos teóricos del liberalismo en la disciplina de relaciones internacionales pueden resumirse en lo siguiente: *1)* un énfasis en la pluralidad de actores internacionales; *2)* la importancia de factores domésticos en el comportamiento de los Estados en el entorno internacional; *3)* el papel de las instituciones internacionales en establecer normas de comportamiento para los actores; y *4)* la expansión de la agenda de estudios internacionales (Eriksson & Giacomello, 2006; Sterling-Folker, 2013).

Si bien es cierto que los liberales están de acuerdo con los realistas en que los Estados son actores centrales en la política internacional, los primeros consideran que estos no son los únicos que pueden jugar papeles significativos en las interacciones internacionales (Keohane R., 1984). Por su parte, la lectura que los liberales dan a la política internacional contemporánea es que la soberanía del Estado-nación constantemente está siendo permeada y fragmentada por el desarrollo de interacciones transnacionales fluidas de actores no estatales (Keohane & Nye, 1977; Khanna, 2016; Eriksson & Giacomello, 2006). Los autores y estudiosos de este enfoque plantean que, aunque para un único actor es complicado desafiar el poder económico, político y militar de un Estado, la creciente red de relaciones transnacionales complejas afecta a los Estados soberanos a tal grado que la *soberanía* se convierte más en un símbolo de integridad territorial que en un activo político sustentable (Keohane & Nye, 1977; Camilleri & Falk, 1992; Rosenau, 1990). Asimismo, el liberalismo recalca que los actores no estatales con capacidad transnacional y económica importan tanto como la seguridad y los Estados (Keohane R., 1984).

En general, el liberalismo tiende a reiterar los resultados positivos de la interdependencia y la interconectividad (Eriksson & Giacomello, 2006, p. 230; (Nye, 2004b). El énfasis se pone sobre las posibilidades de superar los conflictos a través de medios pacíficos, en particular, por medio del establecimiento de normas y la construcción de instituciones a nivel internacional (Finnemore & Sikkink, 1998). A su vez, algunos liberales han apoyado la ampliación de la concepción de seguridad para incluir aspectos económicos, sociales y ecológicos en la definición (Keohane & Nye, 1998). No obstante, paradójicamente, para algunos especialistas "los liberales parecen evaluar el desafío de la revolución de la información tangencialmente" (Eriksson & Giacomello, 2006, p. 231).

De este modo, a través de la revisión de la literatura liberal sobre construcción de regímenes e institucionalización con respecto a la era digital, internet y elementos cibernéticos se puede constatar la poca fertilidad en el terreno. Respecto a temas no relacionados

con la seguridad en el ámbito digital destacan los estudios de Marcus F. Franda (2001) y los trabajos editados por James N. Rosenau y J. P. Singh (2002). A pesar de ello, también existen estudios que bajo este enfoque abordan cuestiones de seguridad en la era digital como los de Lorenzo Valeri (2000) y Giampiero Giacomello (2005). Por su parte, la teoría de la interdependencia compleja ha hecho actualizaciones para adaptarse a los retos planteados por la era digital (Keohane & Nye, 1998; Nye, 2004b). Estos autores argumentan que el "poder suave" se está volviendo más importante en la era digital, principalmente debido a la evolución de múltiples canales de comunicación global que trascienden fácilmente las fronteras soberanas (Keohane & Nye, 1998; Nye, 2004a).

Por otro lado, para algunos analistas, las tecnologías de la información y la comunicación globales no son meramente instrumentos de cooperación, democratización y paz, sino que, a su vez, también pueden ser mecanismos de engaño, propaganda, fraude y terror (Eriksson & Giacomello, 2006; Klimburg, 2017; Morozov E., 2011). Esto puede tener tanto efectos positivos como negativos: por un lado, la integración, la cooperación y la democratización pueden ser más asequibles, pero también el terrorismo, la delincuencia transnacional y la desestabilización de los Estados pueden crecer rápidamente (Eriksson & Giacomello, 2006, p. 232).

Cabe considerar, por otra parte, el enfoque teórico del constructivismo. Este destaca lo ineludible de la interpretación en los fenómenos sociales y, por lo tanto, la distorsión de la realidad, en especial con respecto a la comprensión de la actividad social y política (Adler, 1997; Eriksson & Giacomello, 2006, p. 233). En otras palabras, los constructivistas sostienen que existe una realidad material, así como una realidad social y que es significativo distinguir entre las dos (Wendt, 1999). El argumento central de esta corriente teórica es que, a diferencia de la realidad material, la realidad social se construye socialmente y, por lo tanto, siempre es susceptible de cambiar (Ruggie J. G., 1983; Wendt, 1999). Además, los constructivistas argumentan que la realidad social, así como los intereses y las identidades, nunca pueden ser estáticos o darse por sentado, sino que deben observarse como algo producido y reproducido constantemente (Adler, 1997; Weldes, 1996).

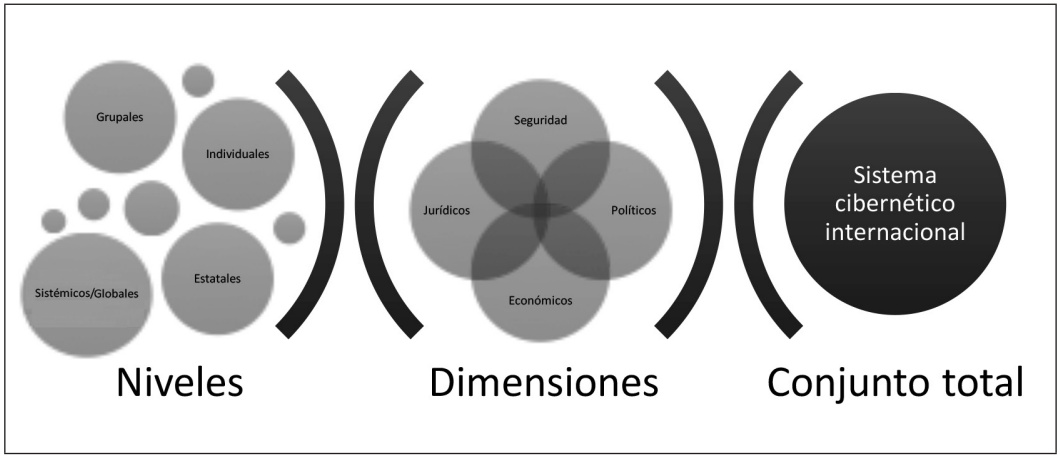
Dentro de este orden de ideas, la teoría constructivista en términos muy generales busca entender qué fuerzas determinan la política mundial o la realidad social (Ruggie, 1998). En el nivel más básico, los actores tienen un conjunto de normas o creencias. Con ello, las normas dan forma a las identidades y, a su vez, las identidades a los intereses, elementos que son vistos como inherentemente dinámicos. Si los intereses cambian, es porque hay un cambio subyacente en las identidades y normas (Adler, 1992; 1997; Ruggie, 1998). Conforme con esta aproximación teórica, los agentes sociales intentarán movilizar las experiencias de otros a través de la configuración de sus intereses para dar forma a la realidad social. Conforme a algunos expertos, eso se ha estado realizando a través de la enmarcación de escenarios catastróficos que se relacionen con experiencias familiares y cotidianas de los individuos para dotar la realidad social con plausibilidad y posibilidad (Hansen & Nissenbaum, 2009).

A. La interrelación entre la política internacional y la seguridad cibernética

Una vez revisadas, de manera somera, algunas perspectivas teóricas de las relaciones internacionales y su visión acerca del desarrollo del paradigma cibernético, es conveniente anotar que la política cibernética cruza un amplio conjunto de áreas temáticas, junto con cambios acordes con el discurso político y con las interacciones, generando efectos mundiales en la articulación y agregación de nuevos intereses, así como nuevos patrones en el escenario internacional, nuevos tipos de respuestas y acuerdos globales (Choucri, 2012, pp. 10-11).

En este aspecto, la política cibernética no es diferente (Valeriano & Maness, 2015, p. 24). Como destaca el politólogo del *Massachusetts Institute of Technology* (MIT) Nazli Choucri (2012, p. 9) "toda política, en la arena cibernética o no, involucra negociación, intercambio y conflicto sobre los mecanismos, instituciones y normas necesarios para resolver de forma acreditada las controversias sobre un conjunto de *valores nucleares* particulares". La siguiente figura busca ejemplificar cómo se ejecutan estos ajustes, en qué niveles se llevan a cabo y cuáles son los efectos, que son multidireccionales, multidimensionales y multinivel.

Figura 2
Política internacional y seguridad cibernética



Fuente: Elaboración propia.

Por otra parte, hay una gran literatura técnica sobre seguridad de redes informáticas, así como una discusión emergente sobre los incentivos económicos y las fallas del mercado que dan forma al problema (Kramer, Starr, Wentz & (eds.), 2009; Lindsay, 2015a; Hansen & Nissenbaum, 2009; Libicki, 2009; Owens, Dam, Lin & (eds.), 2009; Singer & Friedman,

2014). Infortunadamente, el contexto político internacional a menudo se pierde en el enfoque sobre la tecnología y sobre la utilización de esta por grupos especializados. Para algunos estudiosos, la temática de la seguridad cibernética y su impacto sobre la seguridad internacional presenta dos problemas principales para su factibilidad como tópico de estudio sistemático y holístico, tanto dentro de las relaciones internacionales como en el subcampo de los estudios de seguridad internacional (Kello, 2013). El primero se refiere a la escasez de casos disponibles para proponer, probar y refinar afirmaciones teóricas sobre los fenómenos cibernéticos, y el segundo es la tendencia de los gobiernos a clasificar en exceso la información, lo que ha llevado a una brecha de datos significativa, ya que las maniobras tácticas más importantes en el ciberespacio permanecen envueltas en el secreto, lo que complica la investigación académica de los motivos y los objetivos del ataque cibernético como instrumento de política exterior y de defensa (Kello, 2013, pp. 9-10; Schmidt, 2012; Sanger, 2012).

Dentro del subcampo de estudios de seguridad de las relaciones internacionales, en el estado del arte sobre seguridad cibernética, que aún es limitado, la mayoría de análisis presta poca atención a la interrelación de la ciberseguridad con temas políticos, económicos y sociales (Kramer, Starr, Wentz, & (eds.), 2009; Clarke & Knake, 2010; Demchak, 2011; Reveron (ed.), 2012; Libicki, 2007) . Del mismo modo, los analistas de políticas de defensa han dirigido más sus esfuerzos hacia el problema de la interrupción a gran escala de la infraestructura crítica en lugar de prestar atención al desarrollo de interacciones cibernéticas más amplias, transversales y de largo plazo (Lindsay, 2015a, p. 5; Clarke & Knake, 2010; Valeriano & Maness, 2015).

Sin embargo, como recalcan Brandon Valeriano y Ryan C. Maness (2015) en su trabajo, "aquí radica la relevancia de las personas dedicadas al estudio de las relaciones internacionales, puesto que toda acción cibernética tiene una relación directa con la competencia y la rivalidad internacional, ya sea esta interestatal o no"[3]. Por ejemplo, algunos analistas invocan la lógica de Carl von Clausewitz para argumentar que el peligro cibernético es exuberante porque la tecnología (en este caso los medios cibernéticos) no alteran el carácter o los medios de la guerra (Kello, 2013, p. 10; Rid, 2012). Además, otros afirman que los ataques cibernéticos no son violentos y no crean daños colaterales; por lo tanto, los nuevos fenómenos no deben calificarse como actos de guerra o como cuestiones de seguridad internacional (Brito & Watkins, 2011; Dunn Cavelty, 2008b; Liff, 2012; Morozov E., 2009; Rid, 2012).[4]

[3] No obstante que su apunte es una llamada de atención relevante para la comunidad epistémica de la disciplina de relaciones internacionales, su enfoque solo se centra en una cara de las prácticas estatales, el conflicto, dejando de lado el aspecto de colaboración.

[4] En general, estas visiones parten de la definición que otorga sobre la guerra el grupo de investigación *Correlates of War* de la Universidad de Michigan, la cual definen como "un conflicto armado conducido por o entre entidades nacionales, en el que al menos uno de ellos es un estado, en el cual resultan al menos 1,000 muertes en batalla de personal militar" (Valeriano & Maness, 2015).

Por otra parte, hay quienes afirman que habrá una proliferación de la guerra cibernética porque la sociedad digital será una extensión lógica del dominio de seguridad (Rattray, 2001; Clarke & Knake, 2010; Kello, 2013; Nye, 2011). A su vez, otros argumentan que las amenazas cibernéticas y su proliferación son socialmente construidas y que debemos atenuar la elección de la terminología y de las metáforas para su análisis (*cyber war*, *cyber Armageddon*, *cyber 9/11*), pues de esta manera crece la inflación de la amenaza (Hansen & Nissenbaum, 2009).

Asimismo, existen otros factores que condicionan la complejidad del estudio o magnifican la brecha entre lo cibernético y la dinámica internacional. Uno es que la nueva tecnología, en ocasiones es tan especializada que puede impedir la entrada a neófitos tecnológicos (Lindsay, 2015b; Kello, 2013). Por otra parte, está la imbricación de temáticas de diversa índole como delitos informáticos, señales de inteligencia, "guerra electrónica", robo de identidad, protección de la privacidad, estafa electrónica, lo que hace confuso su abordaje, su tratamiento y su análisis (Choucri, 2012; Nye J. S., 2011; Lindsay, 2015a, p. 9).

Dentro del sector académico, algunos observadores afirman que el problema cibernético está plagado de peligros; por ello, cualquiera que intente abordarlo será abrumado por su complejidad (Walt, 2010). Esta postura busca evitar todo diálogo con la cuestión cibernética. De igual manera, un enfoque tradicional que enmarca una idea tradicional de la seguridad y el conflicto internacional, subraya que las amenazas que carecen de un carácter abiertamente físico o que no alcanzan el nivel de violencia interestatal son intelectualmente carentes de interés (Kello, 2013, p. 11; Buzan & Hansen, 2009)[5].

Para algunos, los efectos violentos de una supuesta "guerra cibernética" no necesitan ser letales para caer en la categoría conceptual tradicional de guerra (Stone, 2012, p. 107). Una causa es que hasta finales de la segunda guerra mundial, la guerra se estudió como historia militar o como derecho y filosofía del uso de las fuerzas armadas (Buzan & Hansen, 2009). Por su parte, la geopolítica se centró en cómo la posición geográfica, el espacio y las distancias repercuten en la proyección del poder (Herz, 2013; Kirshner, 2010).

No obstante, existen esfuerzos académicos que realizan compendios sobre las diferentes perspectivas del debate sobre la seguridad cibernética y su relevancia en el entorno de seguridad internacional (Kramer, Starr, Wentz, & (eds.), 2009; Reveron (ed.), 2012; Singer & Friedman, 2014; Valeriano & Maness, 2015; Eriksson & Giacomello, 2007). El debate se puede subdividir en dos grandes perspectivas. Por un lado, una perspectiva sostiene que la infraestructura interconectada hace que las potencias industriales avanzadas sean particularmente vulnerables a serias perturbaciones por parte de los Estados más débiles o incluso de actores no estatales, puesto que las herra-

[5] El estudio de la guerra y de la geopolítica constituyen importantes antecedentes para la preponderancia de este enfoque.

mientas de *hackeo* son cada vez de más fácil acceso (Nye, 2011; Borg, 2005; Brenner, 2011; Clarke & Knake, 2010; Junio, 2013; Kello, 2013; Petterson, 2013; Rattray, 2001).

Del otro lado del debate, distintos analistas argumentan que la industria de la defensa y el *establishment* de la seguridad nacional exageran en gran medida la intensidad de la amenaza cibernética (Dunn Cavelty, 2008b; Lawson, 2013; Ohm, 2008; Brito & Watkins, 2011; Morozov E., 2009; Schneier, 2012). Dentro de este marco, otros afirman que las empresas privadas y actores que operan y gestionan un gran número de sistemas informáticos críticos suelen ser reacios a reportar incidentes cibernéticos perjudiciales debido a su potencial sobrecosto de reputación y de otro tipo (Kello, 2013, p. 10). Por último, otros estudiosos tratan de equilibrar la desacreditación de la retórica exagerada con evaluaciones sobre el potencial de los sustitutos emergentes para la agresión de baja intensidad y los complementos para la guerra de alta intensidad (Betz, 2012; Gartzke, 2013; Liff, 2012; Lindsay, 2013; Libicki, 2007; Rid, 2012).

Junto con este debate sobre la seguridad cibernética (*ciberseguridad*) confluyen, de manera implícita, otros debates teóricos que se engarzan de forma simultánea. Por un lado, un debate sobre el concepto de seguridad, su categorización semántica, su ampliación conceptual, su múltiple dimensionalidad, sus marcos analíticos y la expansión de sus facetas más allá del ámbito militar y de defensa. Por el otro lado, se enlaza un debate acerca de la transición hegemónica internacional y el futuro político-económico debido a la confrontación entre grandes potencias y una posible transformación en el sistema internacional. Por último, las potencias mundiales han comprendido que la protección de la información es un elemento estratégico para la preservación de su dominio y control. Por ello, el análisis del nexo entre estos debates teóricos es imprescindible para comprender el balance entre seguridad del dominio digital, competencia hegemónica y reafirmación o recomposición del *statu quo* internacional y la transformación de las prácticas en esta estructura digital.

CONSIDERACIONES FINALES

Del vacío epistémico detectado proviene la pertinencia y la factibilidad de realizar una mayor investigación en la temática cibernética y sus efectos en el nivel internacional. Bajo este contexto, es evidente la necesidad de estudiar el concepto de ciberseguridad (*seguridad cibernética*) a la luz de las relaciones internacionales, primero para contribuir a la integración de las nuevas realidades cibernéticas en la disciplina, y segundo para analizar la representación de sus efectos sobre la agenda de los estudios de seguridad internacional.

En efecto, el tema de la ciberseguridad internacional es multidimensional, transdisciplinario e incipiente, y por ello difícil de definir con precisión en una forma holística y metódica. Además, es escasamente analizado desde la perspectiva de las relaciones internacionales como se aprecia a lo largo del texto y, por ello, no deja de plantear dificultades el hecho de querer presentar una visión sistémica en torno a una literatura dispersa al respecto y que, además, ilustre cuáles son sus implicaciones sobre la reconfiguración de un orden interna-

cional complejo, imbricado y confuso que ha sido la característica desde la posguerra fría. No obstante, esta propuesta busca incorporar algunos elementos para determinar con mayor precisión cuáles son las razones de la variabilidad en el entorno internacional en relación con las prácticas de seguridad cibernéticas emprendidas particularmente por los actores gubernamentales. La pertinencia de este enfoque radica en la importancia y el tamaño de los actores que ejecutan dicha configuración sobre el debate de la seguridad cibernética, sus características territoriales, demográficas, de poder y, por supuesto, las implicaciones de sus acciones a nivel sistémico en el terreno digital.

REFERENCIAS

Allison, G. T. & Zelikow, P. (1999). *Essence of Decision: Explaining the Cuban Missile Crisis*, 2a. ed., Nueva York: Longman.

Adler, E. (1992). The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the idea of Nuclear Arms Control. *International Organization, 46*(1), 101-145.

Adler, E. (1997). Seizing the Middle Ground: Constructivism in World Politics. *European Journal of International Relations, 3*(3), 319-363.

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy, 12*(2), 141-165.

Beckley, M. (2011). China's Century? Why America's Edge Will Endure. *International Security, 36*(3), 41-78.

Benedikt, M. (1994). *Cyberspace: first steps.* Cambridge, MA: MIT Press.

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed. *Journal of Strategic Studies, 35*(5), 689-711.

Borg, S. (2005). Economically Complex Cyberattacks. *IEEE Security and Privacy Magazine, 3*(6), 64-67.

Brenner, J. (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* Nueva York: Penguin.

Brito, J. & Watkins, T. (2011). *Loving the cyber bomb? The dangers of threat inflation.* Arlington, VA: George Mason University.

Buzan, B. & Hansen, L. (2009). *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Camilleri, J. A. & Falk, J. (1992). *The End of Sovereignty? The Politics of a Shrinking and Fragmenting World.* Aldershot: Edward Elgar.

Castells, M. (2009). *Comunicación y poder.* Madrid: Alianza Editorial.

Choucri, N. (2012). *Cyber Politics in International Relations.* Cambridge: MIT Press.

Clark, D. D. (2010). *Characterizing Cyberspace: past, presente and future.* Cambridge: MIT Press.

Clarke, R. A. & Knake, R. K. (2010). *Cyber War: The Next Threat* . Nueva York: Ecco.

Craig, A. J. & Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. In D. Orsi, J. R. Avgustin, & M. Nurnus, *Realism in Practice: An Appraisal* (pp. 85-101). Bristol, Reino Unido: E-International Relations Publishing.

Crosset, V. & Dupont, B. (2018). Internet et propagande jihadiste: la régulation polycentrique du cyberespace. *Critique Internationale, 78*(1), 107-125.

Deibert, R. J. (2003). Black code: censorship, surveillance, and militarization of cyberspace. *Millennium, 32*(2), 501-530.

Deibert, R. J. (2013). *Black code: surveillance, privacy, and the dark side of the internet.* Toronto: McClelland & Stewart.

Deibert, R. J. & Rohozinsky, R. (2010). Liberation vs Control in Cyberspace. *Journal of Democracy, 21*(4), 43-57.

Deibert, R.; Palfrey, J.; Rohozinski, R. & Zittrain, J. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press.

Deibert, R.; Palfrey, J.; Rohozinski, R. & Zittrain, J. (2012). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press.

Deibert, R.; Palfrrey, J.; Rohozinski, R. & Zittrain. (2008). *Access Denied: the Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press.

Demchak, C. C. (2011). *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security.* Athens: University of Georgia Press.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance.* Cambridge, MA: MIT Press.

DeNardis, L. (2014). *The Global War for Internet Governance.* New Haven: Yale University Press.

Deutsch, K. (1963). *The Nerves of the Government: Models of Political Communications and Control.* Nueva York: Glencoe.

Dobbins, J. (2012). War with China. *Survival, 54*(4), 7-24.

Drezner, D. W. (2009). Bad Debts Assesing China's Influence in Great Power Politics. *International Security, 34*(2), 7-45.

Dunn Cavelty, M. (2008a). *Cyber-Security and Threats Politics: U.S. Efforts to Secure the Information Age.* Nueva York: Routledge.

Dunn Cavelty, M. (2008b). Cyber-terror, looming threat or phantom menace: the framing of the US cyber-threat debate. *Journal of Information & Technology Politics, 4*(1), 19-36.

Ebert, H. & Maurer, T. (2014). Revendications sur le cyberespace et puissances émergentes. *Hérodote, 152-153*(1), 276-295.

Edde, R. (2018). Le droit? Un outil de régulation du cyberespace? Le cas du droit à l'oubil numérique. *Homme et la Societe, 206*(1), 69-94.

Eriksson, J. & Giacomello, G. (. (2007). *International Relations and Security in the Digital Age.* Londres, Nueva York: Routledge.

Eriksson, J. & Giacomello, G. (2006). The information revolution, security and international relations: the (IR) relevant theory? *International Political Science Review, 27*(3), 221-244.

Escobar, A. (06/1994). Welcome to cyberia: notes on the anthology of cyberculture. *Current Anthropology, 35*(3), 211-231.

Fearon, J. D. & Wendt, A. (2002). Realism v. Constructivism: A Skeptical View. In *Handbook of International Relations.* Londres: Sage Publications.

Finnemore, M. & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization, 52*(4), 887-917.

Foot, R. & Walter, A. (2010). *China, the United States, and the Global Order.* Nueva York: Oxford University Press.

Franda, M. F. (2001). *Governing the Internet: The Emergence of an International Regime.* Boulder, CO: Lynne Rienner.

Friedberg, A. L. (2011). *A Contest for Supremacy: China, America and the Struggle for Mastery in Asia.* Nueva York: W.W. Norton.

Friis, K. & Ringsmose, J. (n.d.). *Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives.* Londres: Routledge.

Glaser, C. L. (2004). When Are Arms Races Dangerous? Rational versus Suboptimal Arming. *International Security, 28*(4), 44-84.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41-73.

Gilpin, R. (1981). *War and Change in World Politics.* Cambridge: Cambridge University Press.

Gilpin, R. (1986). The Richness of the Tradition of Political Realism. In R. Keohane, *Neorealism and Its Critics.* New York: Columbia University Press.

Giacomello, G. (2005). *National Governments and Control of the Internet: A Digital Challenge.* Londres: Routledge.

Gibson, W. (1984). *Neuromancer.* Nueva York: Ace.

Goldsmith, J. L. & Wu, T. (2006). *Who Controls the Internet: Illusions of a Borderless World.* Oxford: Oxford University Press.

Goldstein, L. (2015). *Meeting China Halfway.* Washington, DC: Georgetown University Press.

Gourevitch, P. (1978). The Second Image Reversed: The International Sources of Domestic Politics. *International Organization, 32*(4), 881-912.

Hansen, L. & Nissenbaum, H. (2009). Digital disaster: cyber security, and the Copenhagen School. *International Studies Quarterly*(4), 1155-1175.

Herz, M. (2013). Seguridad. In T. Legler, A. Santa Cruz, L. Zamudio (eds.), *Introducción a las relaciones internacionales: América Latina y la política global* (pp. 123-133). México: Oxford University Press.

Ikenberry, J. (2009). Liberal Internationalism 3.0: America and the Dilemmas of World Order. *Perspectives on Politics, 7*(1), 71-87.

Jacques, M. (2009). *When China Rules the World: The End of the Western World and the Birth of a New Global Order.* Nueva York: Penguin.

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics, 31*(2), 289-324.

Johnston, A. I. (2013). How New and Assertive is China's New Assertiveness? *International Security, 37*(4), 7-48.

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate. *Journal of Strategic Studies, 36*(1), 125-133.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace.* New York: Penguin Press.

Kello, L. (2013). The meaning of cyber revolution: perils to theory and statecraft. *International Security, 38*(2), 7-40.

Kennedy, P. (1987). *The Rise and Fall of Great Powers.* Nueva York: Random House.

Keohane, R. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton: Princeton University Press.

Keohane, R. O. & Nye, J. S. (1977). *Power and Interdependence: World Politics.* Boston: Little Brown.

Keohane, R. & Nye, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs, 77*(5), 81-94.

Khanna, P. (2016). *Connectography: mapping the future of global civilization.* Nueva York: Random House.

Kirshner, J. (2010). The Tragedy of Offensive Realism: Classical Realism and the Rise of China. *European Journal of International Relations, 18*(1), 53-75.

Kramer, F. D.; Starr, S. H.; Wentz, L. K. & (eds.). (2009). *Cyberpower and National Security.* Washington, DC: Potomac.

Krauthamer, C. (31/07/1995). Why We Must Contain China. *Time*.

Krishna-Hensel, S. F. (2007). Preface. Cybersecurity: Perspectives on the Challenges of the Information Revolution. In M. Dunn Cavelty, V. Mauer, S. F. Krishna-Hensel (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.* Londres: MPG Books.

Kupchan, C. (2012). *No One's World: the West, the Rising Rest, and the Coming Global Turn.* New York: Oxford University Press.

Lawson, S. (2013). Beyond Cyber-Doom: Assesing the Limits of Hypothetical Scenarios in the Framing of Cyber Threats. *Journal of Information Tehcnology & Politics, 10*(1), 86-103.

Layne, C. (2006). The Unipolar Illusion Revisited: the Coming End of the United States 'Unipolar Moment'. *International Security, 31*(2), 7-41.

Layne, C. (2009). The Unipolar Illusion Revisited: The Coming End of the United States' Unipolar Moment. *International Security, 34*(1), 147-172.

Layne, C. (2009). The Waning of U.S. Hegemony: Myth or Reality? A Review Essay. *International Security, 34*(1), 147-172.

Li, R. (2009). *A Rising China and Security in East Asia: Identity Construction and Security Discourse.* Londres: Routledge.

Libicki, M. C. (2007). *Conquest in cyberspace: national security and information warfare.* Nueva York: Cambridge University Press.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND.

Liff, A. P. (2012). Cyberwar: a new absolute weapon? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies, 35*(3), 401-428.

Lindsay. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404.

Lindsay, J. R. (2015a). The impact of China cybersecurity: fiction and friction. *International Security, 39*(3), 7-47.

Lindsay, J. R. (2015b). Introduction. In J. R. Lindsay, T. Cheung, D. Reveron & (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Area* (pp. 1-26). Nueva York: Oxford University Press.

Mattelart, A. (2007). *Historia de la sociedad de la información.* Barcelona: Paidós.

McEvoy, M. M. (2010). From global village to virtual battlespace: the colonizing of the internet and the extension of realpolitik. *International Studies Quarterly, 54*(2), 381-401.

Mesa, L. (2009). *El debate sobre la seguridad nacional en la República Islámica de Irán. Estudio del primer mandato del presidente hojatoleslam Seyed Mohammed Khatami (1997-2001).* México: El Colegio de México.

Mitrany, D. (1948). The Functional Approach to World Organization. *International Affairs, 24*(3), 350-363.

Moravcsik, A. (1998). *Centralization or Fragmentation? Europe Facing Challenges of Deepening, Diversity, and Democracy.* New York: Council on Foreign Relations.

Moravcsik, A. (1999). *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht.* Londres: UCL Press.

Morgenthau, H. J. (1948). *Politics Among Nations: The Struggle for Power and Peace.* New York: McGraw Hill.

Morozov, E. (2009). Cyber-scare: the exaggerated fear over digital warfare. *Boston Review, 34*(4).

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom.* Nueva York: Public Affairs.

Newitz, A. (16/09/2013). *The Bizarre Evolution of the Word 'Cyber'.* Retrieved noviembre 12, 2018 from Gizmodo: https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487

Nye, J. (2010). *Cyber Power.* Belfer Center for Science and International Affairs, Harvard Kennedy School. Cambridge: Harvard University.

Nye, J. S. (2004a). *Soft Power: The Means to Success in World Politics.* New York: Public Affairs.

Nye, J. S. (2004b). *Power in the Global Information Age: From Realism to Globalization.* Londres: Routledge.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly, 5*(4), 18-38.

Ohm, P. (2008). The Myth of the Superuser: Fear, Risk, and Harm Online. *Univeristy of California Davis Law Review, 41*(4), 1327-1402.

Owens, W. A.; Dam, K. W.; Lin, H. S. (eds.). (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Adquisition and Use of Cyberattack Capabilities.* Washington, DC: National Academies Press.

Palfrey, J. (2010). Four phases of internet regulation. *Social Research, 77*(3), 981-996.

Perrit, H. H. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strenghtening National and Global Governance. *Indiana Journal of Global Studies, 5*(2), 423-442.

Petterson, D. (2013). Offensive Cyber Weapons: Construction, Development, Employment. *Journal of Strategic Studies, 36*(1), 120-124.

Pillsbury, M. (2015). *The Hundred Year Marathon: China's Secret Strategy to Replace America's as the Global Superpower.* Nueva York: Henry Holt.

Rachman, G. (1996). Containing China. *Washington Quarterly, 19*(1), 129-140.

Rattray, G. J. (2001). *Strategic Warfare in Cyberspace.* Cambridge: MIT Press.

Reardon, R. & Nazli, C. (2012). *The Role of Cyberspace in International Relations.* San Diego, CA: ISA Annual Convention.

Reveron, D. S. (eds.). (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington, DC: Georgetown University Press.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 523-544.

Risse-Kappen, T. (1995). *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures, and International Institutions.* Cambridge: Cambridge University Press.

Rosenau, J. N. (1990). *Turbulence in World Politics: A Theory of Change and Continuity.* Princeton, NJ: Princeton University Press.

Rosenau, J. N.; Singh, J. P. (2002). *Information Technology and Global Politics: The Changing Scope of Power and Governance.* Alabany: State University of New York Press.

Ross, R. (1997). Beijing as a Conservative Power. *Foreign Affairs, 76*(2), 33-44.

Ruggie, J. G. (1983). Continuity and Transformation in the World Polity: Toward a Neorealist Theory Synthesis. *World Politics, 35*(2), 261-285.

Ruggie, J. G. (1998). *Constructing the World Polity: Essays on International Institutionalism.* Londres: Routledge.

Russett, B. & Antholis, W. (1993). *Grasping the World Polity: Essays on International Institutionalism.* Londres: Routledge.

Schmidt, M. (13/03/2012). New interest in hacking as threat to security. *The New York Times*.

Schneier, B. (2012). *Liars and Outliers: Enabling the Trust that Society Needs to Thrive.* Indianapolis: Wiley.

Schweller, R. & Pu, X. (2011). After Unipolarity: China's Vision of International Order in an Era of U.S. Decline. *36*(1), 47-72.

Sanger, D. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power.* Nueva York: Crown.

Santa Cruz, A. (2000). *Un debate teórico empíricamente ilustrado: la construcción de la soberanía japonesa, 1853-1902.* Guadalajara: Universidad de Guadalajara.

Santa Cruz, A. (2013). Constructivismo. In T. Legler, A. Santa Cruz & L. Zamudio, *Introducción a las relaciones internacionales: América Latina y la política global* (pp. 36-50). México: Oxford University Press.

Sassen, S. (1998). On the Internet and Sovereignty. *Indiana Journal of Global Legal Studies, 5*(2), 545-559.

Shambaugh, D. (1996). Containment or Engagement of China: Calculating Beijing's Responses. *International Security, 21*(2), 180-209.

Shambaugh, D. (2013). *China Goes Global: the Partial Power.* Nueva York: Oxford University Press.

Shapiro, I. & Wendt, A. (1992). The Difference that Realism Makes. *Politics & Society* (2).

Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs, 90*(1), 28-41.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Nueva York: Oxford University Press.

Snyder, J. (1991). *Myths of Empire.* Ithaca, NY: Cornell University Press.

Starrs, S. (2013). American Economic Power Hasn't Declined- It Globalized! Summoning the Data and Taking Globalization Seriously. *International Studies Quarterly, 57*(4), 817-830.

Steinfeld, E. S. (2010). *Playing our Game: Why China's Economic Rise Doesn't Threaten the West.* Oxford: Oxford University Press.

Sterling-Folker, Jennifer. (2013). *Making Sense of Internationl Relations Theory:* Londres: Lyenne Rienner.

Stone, J. (2012). Cyber War Will Take Place! *Journal of Strategic Studies, 36*(1), 101-108.

Tammen, R. L. (ed.). (2000). *Power Transitions Strategies for the 21st Century.* Nueva York: Chatham House.

Valeri, L. (2000). Securing Internet Society: Toward an International Regime for Information Assurance. *Studies in Conflict and Terrorism, 23*(2), 129-146.

Valeriano, B. & Maness, R. C. (2015). *Cyber war versus cyber realities: cyber conflict in the international system.* Nueva York: Oxford University Press.

Vaidhyanathan, S. (2018). *Antisocial Media.* Nueva York: Oxford University Press.

Van Evera, S. (1997). *Guide to Methods for Students of Political Science.* Ithaca, Londres: Cornell University Press.

Walker, R. B. (1993). *Inside/Outside: International Relations ads Political Theory.* Cambridge: Cambridge University Press.

Walt, S. (1994). The Reinaissance of Security Studies. *International Studies Quarterly, 35*(2), 211-239.

Walt, S. M. (2010). *Is the Cyber Threat Overblown?* Retrieved enero 2, 2018 from Foreign Policy: http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown

Waltz, K. N. (1979). *Theory of International Politics.* Readings: Addison Wesley.

Weldes, J. (1996). Constructing National Interest. *European Journal of International Relations, 2*(3), 335-370.

Wendt, A. (1999). *Social Theory of International Politics.* Cambridge: Cambridge University Press.

Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine.* París: Hermann.

Wu, I. S. (2008). *Information, identity and institutions.* Institute for the Study of Diplomacy. Washington, DC: Georgetown University.

Zittrain, J. (2008). *The future of the internet and how to stop it.* New Haven: Yale University Press.