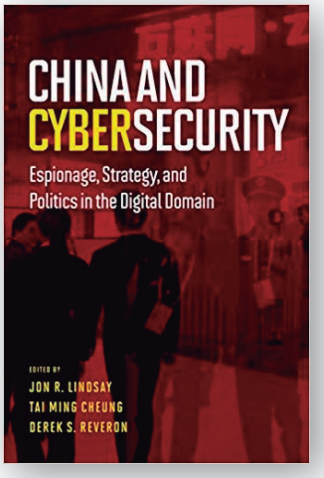
RESEÑA

China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain

DOI: 10.32870/mycp.v8i24.603

Germán Alejandro Patiño Orozco[1]



China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Jon R. Lindsay, Tai Ming Cheung y Derek S. Reveron (eds.), Oxford University Press, Nueva York, 2015.

En la agenda política internacional tanto China como el vocablo ciberseguridad se han convertido en una hipérbole. El desarrollo de internet en China ha sido rápido y completo, no únicamente en términos de cantidad de usuarios y recursos de información en red, sino también en términos de desarrollo industrial e innovación. La evolución de internet ha traído grandes cambios a la sociedad china; en general ha aumentado el acceso a la información y el fortalecimiento de la comunicación. No obstante, junto con la promesa del desarrollo, se derivan posibilidades de riesgo inherentes a la ubicuidad del ciberespacio.

Es precisamente el objetivo central de este libro conjunto, dilucidar cuáles son los puntos y contrapuntos de la seguridad en el ciberespacio y sus implicaciones políticas, económicas y sociales. En el ámbito de estudio de la seguridad internacional, es común señalar que China representa desafíos para el orden internacional. Contrario a lo que es común creer, la tesis principal del libro es que China no es una potencia cibernética ofensiva. Pocos temas liberan tanta susceptibilidad como China y la ciberseguridad, y, aunque se trata de

1. Universidad Autónoma de Baja California (UABC), Facultad de Economía y Relaciones Internacionales, Unidad Tijuana. Calzada Tecnológico y Universidad s/n, Delegación Mesa de Otay, Tijuana, Baja California, México. ORCID: http://orcid.org/0000-0003-0275-0238. Correo electrónico: german.patino@gmail.com

un libro dirigido principalmente a especialistas en los temas de seguridad, desarrollo tecnológico, estrategia militar y derechos de privacidad en línea, los editores y los distintos autores recalcan que lo concerniente a las actividades cotidianas enlazadas a la ciberseguridad constituye una cuestión que afecta a la sociedad global, incluso a aquellos que permanecen lo más alejados posible de cualquier interacción digital.

El texto pretende ofrecer una visión general y de gran alcance sobre las dimensiones multifacéticas de las políticas de seguridad cibernéticas de la República Popular de China; al mismo tiempo intenta establecer los puntos esenciales para el debate de un objeto de estudio escurridizo y paradójico que, por su naturaleza, es opaco y visible, rígido y flexible, pues presenta una alta visibilidad mediática y suma secrecía en la cuestión empírica. Por ello, para algunos estudiosos la temática de la ciberseguridad 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. Los coordinadores de la obra reconocen desde las primeras páginas dicho desafío, por ello es meritoria su pretensión de conjuntar una obra sintética para un tema complejo, intrincado y controvertido. La segunda problemática es la tendencia de los gobiernos a clasificar en exceso la información, lo que ha llevado a una brecha de datos significativa, puesto que las maniobras tácticas más importantes en el ciberespacio permanecen aún envueltas en el secreto.

La obra se divide en 13 capítulos, los cuales a su vez se fraccionan en cuatro grandes secciones. La primera parte, relacionada con el espionaje y el crimen cibernético, brinda una perspectiva general sobre temáticas como la recopilación de inteligencia gubernamental, el espionaje económico realizado por entes públicos y privados, así como las fricciones que ello ha generado en los gobiernos que sufren estas acciones, especialmente el estadounidense. Dentro de este apartado también se evalúan las dimensiones de una economía subrepticia digital. Dentro de esta sección se subraya que la lógica gubernamental china de estas políticas es la estabilidad interna, contrario a la tendencia general, que describe a China como un incitador digital internacional.

En la segunda parte de la obra se aborda la cuestión de las instituciones militares y la estrategia militar en el dominio digital, particularmente las doc-

trinas del Ejército Popular de Liberación, su estructuración en relación con el terreno digital, las unidades encargadas de su ejecución, principios para la movilización en caso de una "guerra cibernética", la formación de algunas "milicias informáticas" y el posible desarrollo de armas virtuales altamente sofisticadas.

Los capítulos 9, 10 y 11, que comprenden la tercera parte del libro, debaten sobre la confluencia y divergencia de intereses en relación con la gobernanza de internet global entre el gobierno estadounidense y el chino. Asimismo, explora tópicos controversiales sobre la formulación de políticas relacionadas con la privacidad y manejo de datos personales en línea, así como el siempre espinoso tema de la censura política digital y su fuerte imbricación con los derechos humanos de libertad de expresión.

En la última sección del texto se ofrecen reflexiones sobre cómo incorporar el estudio de la tecnología a la disciplina de Relaciones Internacionales, las implicaciones prácticas de la competencia internacional de desarrollo tecnológico y recomendaciones para los tomadores de decisiones (principalmente en Estados Unidos) de lo que representa la innovación digital china en el campo de seguridad. De manera implícita, también se encuentran dos debates teóricos que se engarzan de forma simultánea, uno sobre el impacto de la transición hegemónica para la seguridad internacional y el otro sobre el futuro político y económico de una potencia ascendente y la transformación en el sistema internacional, vistos desde la competencia en el terreno digital. Sin embargo, estas controversias son abordadas de forma descriptiva y tangencial, quizá un descuido que se les puede achacar a los coordinadores y autores de la obra.

Como en toda obra colectiva, existen diferencias metodológicas, narrativas, de perspicacia y de observación. Esto puede observarse desde dos lentes distintos: uno, como una debilidad innata del texto, o como una fortaleza, punto que los diferentes colaboradores dejan abierta y a consideración del lector. De esta manera, el libro proporciona un panorama general sobre las consideraciones políticas del Gobierno de la República Popular de China en materia de seguridad cibernética; sin embargo, es importante señalar que en algunos rubros es necesario complementar con otros análisis más profundos que permitan ahondar en el entendimiento de un tema interdisciplinario complejo. El libro es un texto recomendable e indispensable, pues es pionero en su esfuerzo de ofrecer una visión holística de un tópico global que seguirá creciendo en importancia en los próximos años.

Referencias bibliográficas

Kello, L. (2013). The Meaning of Cyber Revolution: Perils to Theory and Statecraft. *International Security*, *38*(2): 7-40. doi: 10.1162/isec_a_00138