Revista 95.1
Revista RELACIONES INTERNACIONALES
Escuela de Relaciones Internacionales.
Universidad Nacional, Costa Rica.
N.º 95.1 • Enero-Junio de 2022
doi: https://doi.org/10.15359/ri.95-1.7
ISSN: 1018-0583 / e-ISSN: 2215-4582 • Pp. 171-175

Reseña del libro: *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* de Ben Buchanan

Valery Brais Chaves[1]
ORCID: 0000-0003-3031-2251

Como si de agregar un nuevo utensilio a una caja de herramientas se tratara, aparece el uso de las habilidades cibernéticas en el plano de la política internacional. Esta es la temática principal del más reciente libro de Ben Buchanan, profesor de la Universidad de Georgetown; su alma máter.

Buchanan tiene un doctorado en Estudios de Guerra por el King's College London. Además, participa del proyecto de seguridad cibernética de la Universidad de Harvard donde realiza investigaciones sobre esta temática y gobernanza. Asimismo, ha escrito artículos sobre inteligencia artificial, ataques cibernéticos, ciberseguridad electoral y propagación de códigos maliciosos (CNAS, 2021).

The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics fue publicado en el 2020, por la Universidad de Harvard, y abarca un periodo desde el 2005 hasta el 2018, tiempo que comprende sucesos como la influencia rusa en las elecciones presidenciales estadounidenses.

La obra está compuesta por 13 capítulos que explican los procesos de las operaciones cibernéticas desde la perspectiva política y, para su comprensión, las divide en tres categorías: el espionaje, el ataque y la desestabilización. Para lograr esto el autor utilizó entrevistas de primera mano, documentación gubernamental, análisis técnicos forenses, documentos filtrados y el estudio minucioso de los informes, por parte de los medios de comunicación.

Todos estos instrumentos, en conjunto con su experiencia académica y profesional, le permiten presentar un libro que exhibe, de una manera muy completa, el funcionamiento de los ataques cibernéticos como un nuevo método de

1 Universidad Nacional, Escuela de Relaciones Internacionales. Estudiante de la Licenciatura en Relaciones Internacionales con énfasis en Política Internacional. Correo electrónico: vale.brais.98@gmail.com

Fecha de recepción: 3 de junio del 2021
Fecha de aceptación: 13 de setiembre del 2021
Fecha de publicación: 17 de enero del 2022

gobernabilidad en las Relaciones Internacionales y que inciden en una nueva normalidad geopolítica.

En cada capítulo expone un caso de ataque cibernético donde los piratas o *hackers*, logran espiar, atacar o desestabilizar a su objetivo. Debido a la naturaleza técnica del tema, el libro trata de ser lo más entendible y claro posible para el público no especializado, por eso utiliza métodos de ilustración como las estrategias de las partidas de póquer, o bien, la analogía de fútbol y del boxeador desde sus primeras páginas.

La primera parte del libro expone las operaciones de espionaje de la agencia de inteligencia estadounidense contra integrantes del Consejo de Seguridad y *La Operación Aurora*, la campaña de espionaje china. Estos casos demuestran que los *hackers* pueden interceptar líneas telefónicas, espiar y alterar la información.

En la segunda parte del libro se explican el ataque perpetuado por Estados Unidos e Israel contra el proyecto nuclear de Irán y la operación *Shamoon*, el ataque realizado por Irán contra la empresa de petróleo Aramco de Arabia Saudita. Irán también fue el autor de la operación *Ababil*, un ataque cibernético contra las corporaciones financieras estadounidenses.

Este segundo apartado, también analiza el intento fallido de coerción realizado por Corea del Norte contra la empresa norteamericana *Sony Pictures Entertainment* y un ataque por *hackers* rusos contra Ucrania, evidenciando que también pueden sabotear, interferir y atacar proyectos estratégicos o de gran importancia para los Estados.

En la tercera y última parte del libro se abarcan los casos más largos y recientes de ciberseguridad, como las operaciones de interferencia en elecciones, en las cuales destacan las infiltraciones de los *hackers* rusos en las computadoras del Comité Democrático Nacional de Estados Unidos y los ataques contra la campaña electoral de Hillary Clinton.

También, se presenta el caso más referenciado del libro, las operaciones de *Shadow Brokers*, un grupo de *hackers* que se adueñó de muchos de los secretos de *The National Security Agency* (NSA) y, además, los multimillonarios robos perpetrados por *hackers* de Corea del Norte en bancos de diferentes partes del mundo. Esto, finalmente, manifiesta que tales individuos, también son capaces de exponer, robar, desestabilizar empresas y países.

Mediante estos casos, Buchanan explica las diferentes formas, técnicas y métodos de infiltración de los *hackers*. Desde el acceso a las bases de datos de las telecomunicaciones hasta códigos malignos y gusanos que llevan los nombres de *Worm cap6, Destover* (caso contra Sony), *Stuxnet and Wiper* (caso contra la NSA), *Shamoon* (ataque de Irán), *WannaCryCode* y *Juniper*; todos estos con la capacidad de infectar millones de computadoras en cuestión de pocos minutos.

Si bien es cierto las operaciones cibernéticas pueden enfrentar algunos obstáculos como el cifrado de los dispositivos, estos son minúsculos en comparación con el daño provocado, así lo menciona el autor:

> Los chinos habían causado al menos treinta mil "incidentes de piratería" en el Departamento de Defensa... Copiaron alrededor de cincuenta terabytes de datos... Obtuvieron acceso a decenas de miles de contraseñas de usuarios militares y decenas de miles de registros de personal, incluidos los de generales y otros altos dirigentes (Buchanan, 2020, p. 77)[2].

En lo que al campo de las Relaciones Internacionales respecta, el libro representa un gran aporte en términos conceptuales por varias razones: visibiliza la presencia de los *hackers* desde hace alrededor de veinte años, como nuevos actores del escenario internacional; determina nuevas necesidades y prioridades, tanto gubernamentales como del sector privado, por obtener programas de actualización de *software*, *scanner* de antivirus, el monitoreo de la red de seguridad, entre otras herramientas orientadas a enfrentar la amenaza constante de ser un posible objetivo de ataque.

Además, el libro refuerza el vínculo entre la geopolítica y la seguridad, prueba de ello es que en los Estados que conforman *The Five Eyes*[3], la mayor alianza de inteligencia del mundo en la cual participa Estados Unidos, tienen en común una ubicación favorable cerca de las costas que les permite alcanzar una cantidad importante de redes telefónicas y telegráficas de manera que pueden cubrir y supervisar prácticamente, todo el hemisferio oriental.

Las capacidades cibernéticas se caracterizan por su naturaleza secreta, el autor menciona que durante años se ha ignorado la manera en que las actividades secretas han modificado el mundo, esto es porque las operaciones solo tienen éxito si los otros Estados no se dan cuenta de lo que sucede. De esta manera,

2 Texto original en inglés: Chinese had caused at least thirty thousand "hacking incidents" in the Department of Defense... They copied around fifty terabytes of data... They gained access to tens of thousands of military users' passwords and tens of thousands of personnel records, including those of generals and other senior leaders (Buchanan, 2020, p. 77).

3 The Five Eyes está conformado por Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos.

Buchanan expone que para gobernar un país se necesitan dos características principales *Signaling and Shaping*, esto significa señalización y modelado; respectivamente.

El libro concluye que, a diferencia de las armas nucleares y los métodos militares como la movilización militar, las operaciones cibernéticas no sirven para la señalización (capacidad para influir e indicar las posiciones de un Estado, para evitar el ataque), por el contrario, explica lo siguiente:

> La mejor manera de conceptualizar las operaciones cibernéticas no es mediante paradigmas centrados en la señalización, sino a través del marco de modelado (*shaping*), arraigado en conceptos como el espionaje, el sabotaje y la desestabilización. Los Estados que cosechan más beneficios de la piratería son los que moldean agresivamente el entorno geopolítico para que llegue a ser más a su gusto, no los que tratan de insinuar, coaccionar o amenazar (Buchanan, 2020, p.10).[4]

Contrario a lo que expresa el libro, la importancia de la esfera digital y cibernética aumenta la brecha entre países como Estados Unidos, que ha creado alianzas con las más importantes compañías telefónicas y ha establecido estaciones en otros países como parte de su política exterior, en comparación con otros Estados que no cuentan con una ubicación propicia ni "con los diez millones de dólares anuales que invierten los países de *The Five Eyes* para mantener e incrementar su dominio en las redes" (Buchanan, 2020, p. 25). Y, aun así, esto puede no ser suficiente para combatir los grupos de *hackers* y su creciente propagación.

En esta caótica arena de operaciones cibernéticas como le llama el autor, el principal actor del libro –después de los diferentes grupos de *hackers*– es *The National Security Agency*, NSA, de los Estados Unidos. Sin embargo, de acuerdo con el texto, siempre se muestra como el actor atacado y no el atacante.

Caso tras caso revela como oponentes de Estados Unidos: Rusia, China, Corea del Norte o Irán realizan ataques contra la NSA o contra otros adversarios; según el libro, los perpetradores de los ataques son *hackers* de grupos criminales y regímenes autoritarios, sin embargo, las operaciones realizadas por la NSA son presentadas como necesarias, por ejemplo, para guiar las estrategias en las

4 Texto original en inglés: *The best way to conceptualize cyber operations is not through familiar signaling-centric paradigms, but through the framework of shaping, rooted in concepts like espionage, sabotage, and destabilization. The states that reap the most benefits from hacking are the ones that aggressively mold the geopolitical environment to be more to their liking, not the ones that try to hint, coerce, or threaten* (Buchanan, 2020, p. 10).

negociaciones, defender a los más vulnerables y, por supuesto, detener las posibilidades de ataques nucleares.

Mediante las operaciones cibernéticas, Estados Unidos puede combatir el crimen y atrapar a los asesinos, sin embargo, los rusos y los chinos las utilizan para obtener información para sobornos, robar grandes cantidades de dinero y generar daños millonarios en las empresas.

Este punto de vista es entendible si se toma en cuenta que el autor testificó ante el Comité Judicial del Senado de los Estados Unidos, con respecto a las operaciones de piratería rusa (CNAS, 2021), y es el encargado de informar periódicamente, a quienes integran el Congreso y su personal, sobre estos actos.

No se puede dejar de lado que *The Hacker and the State Cyber Attacks* es una obra escrita como una herramienta de política exterior estadounidense que representa un valioso aporte para las Relaciones Internacionales, la ciberseguridad, las Ciencias Políticas y la comunicación; al demostrar que todas estas áreas están interrelacionadas en un plano informático secreto.

El libro evidencia que la importancia de la esfera digital radica en ser un espacio donde la red de comunicación global, las compañías de Internet e, incluso, las computadoras personales, se convierten en las armas y los soldados en la cibernética. Estos aspectos son fundamentales para comprender los elementos que pueden amenazar la seguridad de los actores estatales.

Asimismo, representan una crítica a la concepción estatocéntrica de seguridad, enfocada en los gobiernos y el territorio. En definitiva, su lectura es obligatoria para entender que los *hackers* y las operaciones cibernéticas son actores determinantes no solo en la computación, sino en la geopolítica global.

Referencias bibliográficas

Buchanan, B. (2020). *The Hacker and the State Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press. England.

CNAS. (2021). *Ben Buchanan. Center for a New American Security.* https://www.cnas.org/people/ben-buchanan