Lecturas

Cyber Security Politics. Sociot-echnological transformations and Political Fragmentation

Pedroza, Antonela Milagros

Antonela Milagros Pedroza
Universidad Nacional de La Plata, Argentina
Universidad Abierta Interamericana, Argentina

Dunn Calvety Miriam, Wegner Andreas. Cyber Security Politics. Sociot-echnological transformations and Political Fragmentation. 2022. Routledge. Center for Security Studies, Swiss Federal Institute of Technology (ETH). 287pp.. ISBN: 978-0-367-62674-7 (hbk) ISBN: 978-0-367-62664-8 (pbk) ISBN: 978-1-003-11022-4 (ebk)

Relaciones Internacionales
Universidad Nacional de La Plata, Argentina
ISSN: 1515-3371
ISSN-e: 2314-2766
Periodicidad: Semestral
vol. 31, núm. 62, 2022
revista@iri.edu.ar

URL: http://portal.amelica.org/ameli/journal/26/263685019/

En la introducción, los autores afirman que, en el siglo XXI, la Ciberseguridad se ha convertido en uno de los temas más importantes de las agendas securitarias nacionales (Calvety & Wegner, 2022).

Antes de adentrarse en la materia, estos académicos (2022) aclaran que la Ciberseguridad es un problema que se podría denominar ""perverso" debido a que "(...) su naturaleza es transfronteriza, ocurre en múltiples niveles y atraviesa diferentes sectores, entre instituciones, e impacta en todos los actores, tanto públicos como privados, de una manera compleja, interconectada, y frecuentemente en formas altamente politizadas" Calvety & Wegner, 2022, introducción, p.1, citando a Carr & Lesniewska, 2020, p.392).

Esta definición aparenta ser abarcativa, siguiendo a Calvety y Wegner (2022), debido a que de ella se desprenden dos clases de problemas. El primero de ellos es que los problemas perversos (wicked problems, en inglés) no admiten definiciones cerradas y el segundo es que su resolución presenta como compleja porque involucra a una gran variedad de grupos de interés que a menudo tienen intereses divergentes, con lo cual se vuelve difícil que una solución pueda conformar a todos ellos.

Nuestros autores catalogan a la ciberseguridad como un problema políticamente relevante porque en él se entrecruzan el desarrollo tecnológico acelerado, las estrategias políticas de los sectores estatal y público y los intentos de estos dos y de las burocracias de definir límites y responsabilidades. En este sentido, el libro de referencia es un intento declarado de los autores de abordar las diferentes facetas del problema y sus implicancias (Ibidem)

A fin de definir el objeto de estudio, Calvety y Wegner (2022) establecerán que el "ciberespacio" es un sistema sociotécnico complejo. En este sentido, realizarán tres aclaraciones relevantes, que echarán luz al lector para poder abordar el resto de la lectura. La primera, se trata de un problema políticamente sensible porque el ciberespacio es posible por la tecnología creada por el ser humano y porque es influenciado por fuerzas económicas. Segundo, el ciberespacio está interconectado con otros sistemas como la red energética, infraestructura, comunicaciones y distintos servicios, En este sentido, cabe recordar las elecciones políticas estadounidenses del año 2016 para tomar magnitud del problema. Tercero, el ciberespacio está constituido por tecnología y sus operadores humanos en una interacción que se complejiza cada vez más y que da lugar a problemas que van desde fallas internas a ciberataques externos, por lo cual, para estos autores (2022), los seres humanos son tanto parte del problema como de la solución (introducción, p.2)

Partiendo del problema que se presenta al intentar definir el término "seguridad", debido a sus implicancias nacionales e internacionales, estos dos expertos (2020) lo denominarán un concepto en disputa y afirmarán que dicho inconveniente se trasladará al concepto de Ciberseguridad. En concreto, el término "seguridad" será considerado como polisémico debido a que habrá tantas definiciones como comunidades. El concepto que ofrecerán, por lo tanto, será el siguiente: "(...) se refiere a las actividades ofensivas y defensivas del Estado y de los actores no estatales en el ciberespacio, que sirvan al propósito de ampliar los objetivos políticos securitarios mediante la explotación de oportunidades a ellos relativas." (introducción, p.3)

Es dable señalar, en este punto, que "El principal objetivo del libro es retratar cómo los desarrollos tecnológicos interactúan con dinámicas sociopolíticas y socioeconómicas más amplias a fin de clamar por respuestas diferentes en las políticas nacional e internacional." (Calvety y Wegner, 2022, Introducción, p.4)

Así, los dieciséis capítulos que comprende este libro tienen como base una comprensión de las políticas de ciberseguridad como

"(...) un interjuego entre las tecnologías digitales, sus desarrollos, sus usos y mal usos por los actores humanos en contextos económicos, sociales y políticos conflictivos, y enfrentando procesos de negociación entre actores políticamente relevantes respecto de sus roles y responsabilidades respecto de reglar este problema". (Calvety y Wegner, 2022, Introducción, p.4)

De este modo, los académicos (2022) reconocen dos dimensiones en el problema de la ciberseguridad, una doméstica y otra internacional. En esta última, es decir, en la arena internacional, los estados intentan darle a la ciberseguridad la forma que se condice con sus objetivos estratégicos, mientras, al mismo tiempo, intentan generar estabilidad mediante el establecimiento de reglas de comportamiento. En el otro plano, en el nacional, el estado y su burocracia negocian con el sector privado y la sociedad civil respecto de las libertades y responsabilidades que le corresponden a cada quien.

En suma, este tomo incluirá asuntos nacionales e internacionales, a actores estatales y no estatales, perspectivas políticas, sociales, económicas, técnicas; todo ello debido a la ya mencionada complejidad del tópico a tratar: la ciberseguridad.

El libro editado por Colvelty y Wegner (2022) consta de dos partes y de dieciséis capítulos, escritos por diferentes autores. Mientras que en la primera parte se abordan los cambios sociotécnicos y sus implicancias para la acción política, la segunda se enfoca en la respuesta política a dichos cambios.

En los capítulos de la primera parte del libro se hace foco en la ciberseguridad como telón de fondo de la fragmentación política, la escalada de tensiones geopolíticas y los desacuerdos a nivel internacional respecto de qué conducta debe o no aceptarse en el ciberespacio. En este punto, los editores de este libro (2022)

se preguntarán por la relevancia de las operaciones de ciber-influencia, por su impacto y por sus efectos potencialmente desestabilizadores.

En un intento de dar respuesta a estos interrogantes, Baezner y Cordey (2022), en el primer capítulo, harán un recorrido por las principales tendencias y actores ciber-securitarios y cómo éstos explotan las zonas grises en ambos niveles, doméstico e internacional. Así, a nivel internacional, países como China, Rusia, los Estados Unidos, Corea del Norte, utilizan la ciberseguridad como herramienta alternativa a la guerra (para evitar conflictos que puedan escalar y que los coloquen en un lugar de desventaja logística y de capacidades militares, y debido a la accesibilidad de ciberarmas y de que se encuentran normativamente en una zona gris) a fin de perseguir sus intereses políticos y económicos.

En el capítulo 3, Schünemann (2020) intenta entender el fenómeno y su impacto político a través de las operaciones de influencia y su efecto desestabilizador para los gobiernos democráticos. La novedad ofrecida por el autor radica en tomar fenómenos tales como la automatización y analizar su influencia en las campañas de desinformación e influenciación.

En el capítulo 4, Haunschild, Kaufhold y Reuter (2022) toman los conceptos de violencia y paz naturales para mostrar cómo las noticias falsas (fake news) y la propaganda terrorista aportan a la fragmentación política mediante la utilización de los medios masivos de comunicación. Para ellos, la tecnología amplifica los efectos de estas tendencias mediante, por ejemplo, los social bots.

En el capítulo 5, Bonfanti (2022) trae a colación la relación entre inteligencia artificial y ciberseguridad, y plantea interrogantes respecto a los efectos en la gobernanza de esta tendencia creciente. En este sentido, el autor esboza que los resultados de dicha gobernanza se verán influenciados por la calidad de la relación de los actores involucrados (Estado, organizaciones privadas, sociedad civil) y su capacidad de llegar a acuerdos.

En el capítulo 6, Lindsay (2022) muestra la dinámica paradójica de la criptología y la ciberseguridad. La autora afirma, en este sentido, que son las decisiones políticas y no la tecnología la que complejizan el contexto en el que se desenvuelve dicha tendencia y la vuelve una amenaza a la estabilidad de la estrategia ciber-securitaria.

En el capítulo 7 Eriksson y Giampiero Giancomello (2022) ponen su atención en la expansión de la infraestructura de ciberseguridad, esto, no en cuanto a la infraestructura en sí sino en cuanto a los efectos del cambio tecnológico en la política: en la gobernanza, en el poder, en la rendición de cuentas, entre otros. Los autores señalan cómo la multiplicación y multiplicidad de actores es la que genera más incertidumbre y fragmentación política.

Adentrándonos ya en la parte 2, el capítulo 8, Gómez y Whyte realizan un aporte behaviorista, los autores (2022) analizan las respuestas cognitivas y la toma de decisiones por parte de países tales como Taiwán, Estados Unidos, Filipinas a ciberataques en casos de juegos de guerra internacionales. Valorizan, de esta manera, cómo las perspectivas cruzadas de los actores llevan a determinados resultados. El contexto de estos razonamientos serán las rivalidades geoestratégicas existentes en el mundo. En la misma línea, en el capítulo 9, Lupovici (2022) analiza la dimensión de la ciberseguridad en los nuevos desarrollos del conflicto árabe-israelí.

Los tres capítulos siguientes cambian el foco hacia los problemas geopolíticos que genera la ciberseguridad en tres Estados diferentes: Steiger (capítulo 10) se refiere a la política cibersecuritaria alemana, poniendo su atención en la problemática de la legitimidad del establecimiento de políticas públicas al respecto. El autor Brantly (capítulo 11), por su parte, se ocupará del caso ucraniano en torno a la construcción de estructuras que permitieran la resiliencia cibersecuritaria con ayuda de sus aliados europeos y de la OTAN. Jusufi (capítulo 12) explica el problema del cibercrimen en Albania en detrimento de la estrategia nacional securitaria, debido a amenazas externas e internas relacionadas a actores no estatales.

Los tres últimos capítulos abordan la opacidad en la temática del comportamiento político en el ciberespacio, teniendo en cuenta al actor estatal y al no estatal. Eggenschwiler (capítulo 13) analiza la influencia de estos dos tipos de actores en el modelado de las cibernormas, especialmente de las corporaciones tecnológicas. El investigador Steed (capítulo 14) estudia cómo las agencias de inteligencia profundizan los

problemas de fragmentación política, generando así "ciberinseguridad" (p.186). En el capítulo 15, Kuerbis; Badiei, Grindal y Mueller (2022) piensan cómo podría lograrse más gobernabilidad en el ciberespacio mediante una "institucionalización transnacional" (introducción, p.10)

Wenger y Calvety, en la conclusión y capítulo 16, retoman algunos de los temas señalados por otros autores en capítulos anteriores y a lo largo del libro, a fin de exponer algunos puntos principales y conclusiones que de ellos se desprenden. Primero que nada, la limitación de las ciberoperaciones, expuestas al sabotaje a la subversión. Segundo, el rol de los actores privados en temas de ciberseguridad, de las instituciones públicas, la carrera tecnológica y las ciberamenazas. En tercer lugar, la ciberamenaza como un fenómeno multidimensional que no permite tomar decisiones que generen estabilidad y certeza. Cuarto y último, los autores dejan planteado el problema de cómo superar la fragmentación de la autoridad y la falta de rendición de cuentas.

A fin de cuentas, se trata de un libro que nos plantea cómo la tecnología está cambiando la vida social y política, sin dejar de lado la codependencia y la coconstrucción de la tecnología y la política (Wenger y Calvety, 2020, p.10).