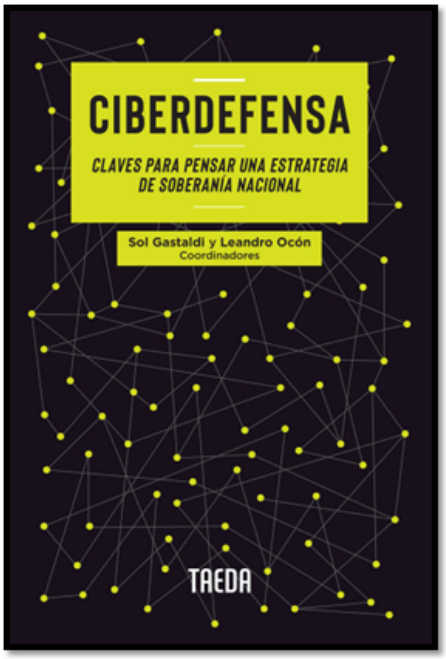
Reseña del libro *Ciberdefensa: claves para pensar una estrategia de soberanía nacional* de Sol Gastaldi y Leandro Ocón (2020)*

https://doi.org/10.22395/csye.v12n23a22



Portada del libro *Ciberdefensa: claves para pensar una estrategia de soberanía nacional.*

Fuente: Gastaldi, S. y Ocón, L. (2020).

Jorge R. Kravetz
Universidad de la Defensa Nacional, Buenos Aires, Argentina
jkravetz@gmail.com
https://orcid.org/0000-0003-3884-5407

* Cómo citar: Kravetz, J. (2023). Reseña del libro *Ciberdefensa: claves para pensar una estrategia de soberanía nacional* de Sol Gastaldi y Leandro Ocón (2020). *Ciencias Sociales y Educación*, *12*(23), 475-481. https://doi.org/10.22395/csye.v12n23a22
Recibido: 8 de noviembre de 2022.
Aprobado: 18 de noviembre de 2022.

En el contexto de la aparición en el Siglo XXI de una nueva dimensión de la seguridad estadual ligada al desarrollo del ciberespacio, y fruto del trabajo de un grupo de investigadores argentinos de la Universidad de la Defensa Nacional (UNDEF) especializados en temas de ciencia política, relaciones internacionales, geopolítica, seguridad y defensa, es que nace este proyecto de investigación académico orientado a dar luz sobre las reflexiones y los debates más actuales en materia de desarrollo de estrategias y políticas de ciberdefensa. Los coordinadores de este proyecto han logrado presentar un trabajo final bien integrado y con una eficaz organización temática, en donde todos los participantes del proyecto han podido plasmar el resultado de sus investigaciones en los distintos capítulos que conforman esta obra.

Este libro comienza con un atrayente prólogo escrito por el ex-Director y fundador de la Autoridad Nacional de Ciberseguridad del Estado de Israel en 2016, Baruch Carmeli, quien describe de manera detallada la evolución en los últimos años de los problemas de seguridad en el ciberespacio y como los organismos de defensa de su país debieron ir adaptando su enfoque tradicional, orientado casi exclusivamente a la protección de datos, por uno nuevo que considere, además, la forma en que operan los atacantes cibernéticos. De manera interesante narra el autor como nació en su país el organismo encargado de la seguridad del Estado en el ciberespacio y los desafíos con los que se encontró al liderar esta nueva organización estadual.

El aporte más sobresaliente de este punto es en el cual el autor describe, en forma detallada, el modelo de gestión de nueve bloques implementado exitosamente por esta organización gubernamental israelí. Este modelo se basa en una amplia gama de actividades y procedimientos que abarcan temas operativos, tecnológicos, de desarrollo del capital humano, de inteligencia, de sinergia con otras organizaciones, de cooperación internacional, de legislación y de cooperación con medios de comunicación. En síntesis, este novedoso modelo de gestión aquí presentado posee información valiosa que cualquier otro Estado nación podría tomar como marco de trabajo para la definición o mejora de la propia gestión y gobernanza de sus organismos vinculados a la protección del ciberespacio.

A este muy interesante prólogo lo sucede una introducción, elaborada por Sol Gastaldi, directora del proyecto de investigación, que nos prepara para los seis capítulos siguientes del libro. En este punto se nos pone en contexto sobre algunas problemáticas ligadas al desarrollo del "ciberespacio" y las reflexiones de diversos autores respecto a su utilización con fines estratégicos por parte de distintos actores del sistema internacional, su impacto en la llamada "Revolución de los Asun-

tos Militares", los tipos de ciberconflictos que podríamos esperar que se sucedan en el futuro, y las dificultades para administrar la soberanía nacional por parte de los Estados en este espacio. Es valiosa, además, la contribución de la autora al plantear diversos debates teóricos sobre algunas cuestiones como, por ejemplo, el alcance de la ciberguerra, la utilización del ciberespacio como medio para confrontar o desestabilizar un oponente, el ciberespacio como vía alternativa a la diplomacia y a la guerra para lograr objetivos políticos, o su utilización como medio para otras actividades como disrupción, espionaje o degradación.

En el primer capítulo, escrito por Leandro Ocón codirector del proyecto, tenemos un eje temático centrado en la "espacialidad del ciberespacio", es decir, en comprender cual es la relación del ciberespacio con el mundo físico, ya que a partir esta conceptualización espacial es que se podrán elaborar y consecuentemente resolver, interrogantes en temas de ciberseguridad o ciberdefensa. Sobre este análisis del ciberespacio y el mundo físico quizás está uno de los mayores aportes del capítulo en el que se plantea una original idea acerca de ver al ciberespacio como un espacio de relacionamiento cognitivo basado en una esfera lógica y una física, que influye tanto en las dinámicas sociales como en el funcionamiento de dispositivos físicos.

Asimismo, se propone aquí, un modelo de cuatro capas, basado en el modelo de Libicki (2009) para relacionar al ciberespacio con el mundo físico, relación que permite ver que acciones en el ciberespacio pueden tener efectos en el mundo físico. Es por ello, plantea el autor, que el ciberespacio es un espacio intrínsecamente geopolítico, y por ende se pregunta si éste es un espacio que puede ser entendido como un nuevo dominio militar al igual que la tierra, mar, aire y espacio. Una vez expuesto este importante interrogante ahonda en un muy atractivo debate que distintas corrientes teóricas, en ocasiones antagónicas, proponen para intentar responderlo.

En el capítulo siguiente, escrito por Rodrigo Cárdenas Holik, se cambia este enfoque teórico y geopolítico del ciberespacio, propuesto en el capítulo anterior, por uno más técnico centrado en mostrar la evolución y las interrelaciones entre los elementos tecnológicos que lo conforman, como lo son el hardware, el software, sistemas de comunicaciones o redes, y los usuarios. En este trabajo el autor realiza un interesante repaso histórico y evolutivo de los componentes tecnológicos que forman parte del ciberespacio, y en donde a la vez, pone sobre relieve la idea de la extrema dependencia del hombre con el mundo cibernético planteando que no hay tarea, acción, operación o fin que no tenga, como intermediario, un dispositivo creado por el

hombre para facilitar distintas actividades, y que estos dispositivos contienen componentes que pueden ser vulnerados.

El punto clave, plantea el autor en forma de advertencia, respecto a los problemas de seguridad de la información en el ciberespacio, no es si van a existir, sino "cuando" van a suceder. Con relación a estas vulnerabilidades, nos muestra este capítulo, los importantes desafíos que deben considerar los decisores de las organizaciones, tanto públicas como privadas, en cuanto a los requerimientos de confidencialidad, integridad y disponibilidad de la información. Se aporta aquí información detallada sobre cómo actúan los atacantes, que abanico de ciberarmas utilizan, y nos describe también, algunas de las estrategias metodológicas más conocidas para hacer frente a los posibles incidentes de seguridad o ciberataques dentro de las organizaciones.

El tercer capítulo, escrito por Sol Gastaldi y Camilo Gioffreda, se centra en un meticuloso análisis de los dilemas estratégicos que presenta el ciberespacio para los Estados nación. Esta visión estratégica del ciberespacio se desprende de la concepción de que este es un medio de proyección de poder en el cual los actores pueden lograr objetivos políticos a través de su utilización Plantean, acertadamente, desde la perspectiva de una víctima estadual de un ciberataque, tres interrogantes que se deben responder: ¿Quién?, ¿Dónde?, ¿Qué acción tomar?

A estos tres interrogantes los conectan en forma directa con tres dilemas. El primero es el dilema de la atribución en el ciberespacio, para el cual nos presentan el abordaje de distintas corrientes teóricas que nos muestran que si bien es un dilema difícil de resolver no es imposible. El segundo dilema tratado es en referencia a los alcances de la asimetría en el ciberespacio, en donde actores, estaduales o no, con pocos recursos pueden atacar a Estados nación más poderosos e infligirles daño. Nos aporta aquí, además, el análisis de la conexión de la asimetría con la "hibridez" o con la posibilidad de combinar por parte de un atacante medios militares convencionales con ciberataques. El tercer dilema planteado es el de la relación del ciberespacio con la esfera pública y privada, o con la dificultad que tienen los Estados para materializar una estrategia de asociación entre ambas esferas en lo relativo a la protección de las infraestructuras críticas, que son un elemento clave del escenario estratégico. El cuarto y último dilema abordado es el del vació legal internacional respecto a este nuevo dominio, y como este vació jurídico incrementa la incertidumbre de los Estados y potencia la anarquía del sistema internacional.

El cuarto capítulo Sol Gastaldi y Sergio Eissa analizan el fenómeno del ciberespacio desde el punto de vista de las relaciones internacionales. Aquí profundizan en los aportes y las limitaciones de las principales escuelas de las relaciones internacionales y a la vez intentan identificar algún otro enfoque específico para el ciberespacio. En primer lugar, para ponernos en contexto, los autores realizan un repaso teórico de las principales características del realismo, el liberalismo, y el constructivismo, para luego sí, plantear el abordaje del ciberespacio.

Por medio de este valioso análisis los autores demuestran que no hay abordajes conclusivos sobre la cuestión ciberespacial, y se preguntan si este fenómeno no requiere de nuevas teorías que fusionen escuelas, o que planteen abordajes más pragmáticos. Es en este punto en dónde encontramos uno de los aportes más valiosos del capítulo ya que luego de analizar y evaluar distintos aspectos teóricos centrales como la percepción de niveles de ciberconflictos, la espacialidad del ciberespacio, el dilema de la atribución, la militarización del ciberespacio, las características del ciberespacio como dominio militar y el desarrollo de la táctica, nos preanuncian que estamos en la génesis de dos nuevos enfoques o corrientes teóricas opuestas frente a cuestiones estratégicas clave del ciberespacio.

En el quinto capítulo, Araceli Díaz, Elio De Antoni y Claudio Robelo Guzmán, nos presentan un análisis empírico de las experiencias desarrolladas por tres países referentes para la República Argentina en materia de ciberdefensa y ciberseguridad, con el objetivo de compararlas y obtener sus similitudes y diferencias. Es decir, se abandonan aquí las cuestiones teórico-conceptuales para sumergirse en un estudio comparado de casos que evalúa cuestiones clave como el marco normativo, las consideraciones estratégicas y la organización operativo-institucional en materia de ciberdefensa y ciberseguridad entre los Estados Unidos, España y Brasil.

Este estudio comparado nos describe con claridad, entre otras cosas, como cada uno de éstos países ha interpretado el ciberespacio, como lo han incluido en la su agenda de seguridad nacional, qué herramientas utilizaron para resolver los problemas tecnológicos, cómo han separado la ciberdefensa de la ciberseguridad, cuál es grado de correlación que poseen entre su política exterior y su estrategia de ciberseguridad y/o ciberdefensa, como gestionan las ciberamenazas, como realizan la complementación público-privada y que estructuras militares utilizan. Además, este detallado análisis, es una valiosa herramienta que podría ser utilizada como base de conocimiento para cualquier otro decisor en la materia dado que está basado en datos de la experiencia empírica de tres países de relevancia en occidente.

En el último capítulo de la obra, Alfredo Leandro Ocón, Federico Verly y Ana Albarracín Keticoglu indagan sobre la cuestión de la soberanía en el ciberespacio, es decir, sobre la facultad de una autoridad de ejercer su poder y control sobre un territorio determinado y se preguntan: ¿cómo se puede trasladar el concepto de territorialidad de la soberanía a un espacio virtual? Para responder este interrogante recorren un profundo camino de análisis teórico, en el cual indagan sobre el concepto de soberanía y su evolución a lo largo de los años. Analizan también la construcción política de soberanía sobre la base de políticas de defensa y seguridad como principal mecanismo de ejercicio de poder soberano de un Estado, revisan como incide el ciberespacio en la autonomía de los Estados, abordan la problemática o las tensiones que se generan entre la interdependencia y la autonomía en un mundo globalizado y como se han materializado las políticas de ciberseguridad y ciberdefensa de los Estados, para finalmente reflexionar acerca del poder en el ciberespacio como mecanismo de ejercicio de la soberanía nacional.

Encontramos también en este punto otros valiosos debates sobre nuevos dilemas y desafíos relacionados a la definición y alcance del ciberespacio, su realidad o virtualidad, si es un dominio específico o transversal a otros dominios como tierra, mar, aire, o espacio exterior o si, por otro lado, es todo a la vez. Asimismo, se preguntan si el ciberespacio es parte de un nuevo sistema global que ha evolucionado, y en el cual para los Estados soberanos no es ya necesaria la exclusividad ni la territorialidad.

En síntesis, a lo largo de los capítulos los investigadores han logrado mediante análisis teóricos y empíricos reflexionar, entre otras cosas, sobre las características y orígenes del ciberespacio, plantear los dilemas de su naturaleza tecnológica, espacial y estratégica para los Estados, analizar el desafío que representa el ciberespacio para la cuestión de la soberanía estatal, y en este sentido recorrer el abordaje que han hecho distintos Estados nación para fortalecer, ampliar o generar soberanía en este espacio. Por lo tanto, este libro nos presenta, sin lugar a duda, los debates, reflexiones y teorías más actuales entorno a este nuevo dominio y aborda temas poco explorados por la academia en la actualidad, que pueden ser de gran aporte y utilidad tanto para investigadores como para decisores en la materia.

Referencias

Gastaldi, S. y Ocón, L. (2020). *Ciberdefensa: claves para pensar una estrategia de soberanía nacional.* TAEDA

Libicki, M. (2009). *Cyberdeterrence and Cyber War.* RAND Corporation.