EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 1, número 2, julio-diciembre 2022
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

Reseña de libro. La ciberseguridad, sus impactos y desafíos

Book review. Cybersecurity, its impacts and challenges

Viviana Pilar Fuquen Flautero

CITACIÓN APA:

Fuquen Flautero, V.P. (2022). Reseña de libro. La ciberseguridad, sus impactos y desafíos. *Ciberespacio, Tecnología e Innovación, 1*(2), 195-197.
https://doi.org/10.25062/2955-0270.4801

Publicado en línea: **Diciembre 30 de 2022**

Enviar un artículo a la Revista

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 2, julio-diciembre 2022 (pp. 195-197)
Bogotá, D.C, Colombia

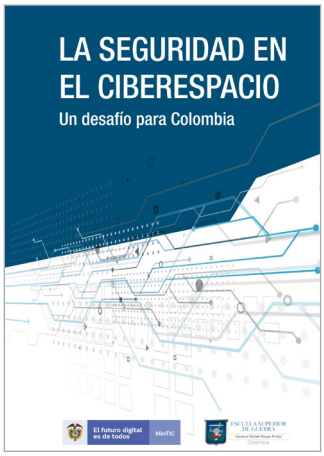
EDITORIAL **ESDEG**

Reseña de libro. La ciberseguridad, sus impactos y desafíos

Book review. Cybersecurity, its impacts and challenges

DOI: https://doi.org/10.25062/2955-0270.4801

Viviana Pilar Fuquen Flautero
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia



Autores del libro: **René Leiva Villagra, Hernán Díaz Mardones, René Leiva Villagra, Mario Arteaga Velásquez, Carl Marowski Pilowsky y Mario Polloni Contardo**
Editorial: Centro de Estudios Estratégicos CEEAG
Año: 2018
ISBN impreso: 978-956-7734-09-2
Páginas: 168

El libro *La ciberseguridad, sus impactos y desafíos* es una compilación de siete capítulos de diferentes autores que abordan la transformación de la guerra en el ciberespacio, un ambiente complejo que cada vez despierta más el interés de expertos y académicos en el ámbito militar, también resulta ser un nuevo eje de investigación en Centro de Estudios Estratégicos de Chile, una institución que es referente en el ámbito estratégico defensa.

En el primer capítulo titulado *Aparece la ciberguerra* se abordan las bases de la ciberguerra. En este se abordan los aspectos conceptuales del ciberespacio y cómo se proyectan desde una visión estratégica moderna, dónde el usuario, la infraestructura, los protocolos y los sistemas operativos interactúan a la par del desarrollo tecnológico. Como ideas principales, se establece la transformación de la guerra, lo cual implica

transformar el pensamiento tradicional y contemplar medios y métodos para desarrollar un conflicto desde el ámbito ciberespacial.

En el segundo capítulo, *Infraestructura crítica vulnerable a la ciberguerra*, afirma que existen unas ventajas y unas oportunidades en el ámbito de la información y las telecomunicaciones, pero en el ciberespacio donde todo interactúa como una red de interconexión que requiere, necesariamente, de infraestructura crítica entendida como las capacidades técnicas y organizacionales relacionadas con activos estratégicos y que son importantes para la sociedad.

Entre los aspectos importantes a señalar en este apartado, se encuentra que la ciberguerra, en los últimos años, ha convertido la infraestructura crítica en un objetivo estratégico para las naciones que pueden desarrollar hostilidades en el ciberespacio, por tal motivo se requiere el desarrollo e instalaciones, redes, servicios y equipos físicos de alta tecnología que se encuentran articuladas en una estrategia de seguridad nacional desde el ciberespacio, esto con el objetivo de contener las amenazas y reducir los riesgos a infraestructuras importantes como la energética, los servicios financieros, la seguridad pública, el transporte y la defensa.

En tercer capítulo, *La lógica de la ciberguerra y su relación compleja con la disuasión*, en este escrito se analiza de manera crítica lo que significa la complejidad de las amenazas y el riesgo que se generan a través del ciberespacio. Conceptos como ciberdefensa y ciberseguridad son el motivo de análisis en este apartado, reconociendo que son dos ámbitos que se complementan para mantener la confiabilidad, integridad y disponibilidad de la información a manera de una *tríada*. Adicionalmente, se resaltan las múltiples amenazas que existen en la red, destacando que también existen unos riesgos relacionados con la infraestructura y las capacidades tecnológicas de los Estados. Como conclusión, se afirma que el ciberespacio se está consolidando como un factor estratégico que requiere que el campo de la defensa oriente una estrategia de seguridad y desarrolle medidas de prevención, disuasión, protección y reacción de la ciberdefensa.

El cuarto capítulo, *El desafío del combate por el mando y control,* analiza dos conceptos importantes en el desarrollo de las hostilidades: El mando y control. Es importante que exista un desarrollo doctrinal debido a que existe una creciente necesidad de contener amenazas y riesgos generados por las diferentes tipologías de guerra entre las cuales se destaca la guerra electrónica y la guerra de la información. Es por esto que en el marco del desarrollo de las operaciones de combate debe existir el mando y el control, entendiendo que existe un quinto dominio de la guerra basado en la información y en donde se deben establecer estrategias defensivas y ofensivas.

El quinto capítulo, *Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica*, se realiza un importante análisis sobre los efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica. Complementando los análisis

anteriores, en este apartado se resalta el efecto que puede causar la guerra en el ciberespacio a la infraestructura crítica, afirmando que existe un alto nivel de riesgo para una nación si la infraestructura es atacada, especialmente, infraestructuras que dependen de sistemas de información y comunicaciones. En consecuencia, y bajo la lógica de la intercomunicación en el ciberespacio, existen responsabilidades de ciberdefensa y ciberseguridad que son transversales, por tanto, las capacidades operacionales de la guerra deben identificar y contrarrestar los diferentes riesgos y amenazas en los diferentes campos civiles y militares.

El sexto capítulo, *El Derecho Internacional como marco regulatorio de la ciberguerra*, y sin dejar de lado el marco jurídico, este apartado aborda el alcance jurídico que debe desarrollarse mediante políticas y marcos regulatorios internacionales enfocados al ciberespacio. Demostrando la existencia jurídica de regular el enfrentamiento o conflicto desde un nuevo escenario de guerra. Se resalta las bases generadas en el *Manual de Tallínn*, afirmando que pueden ser insumos para considerar el derecho de defensa de un Estado ante ciberataques.

Finalmente, el capítulo *Desafíos para afrontar la ciberguerra Equipo CEEAG*, este apartado aborda el debate sobre los desafíos a afrontar a largo plazo por parte de los Estados. Se establece que existen ejes fundamentales que deben desarrollarse para contener las amenazas, los riesgos del ciberespacio y se encuentran enmarcadas en competencias, capacidades y nivel madurez de los sistemas de información y organizacionales para generar respuesta ante incidentes. Si bien todos los riesgos o amenazas pueden afectar la infraestructura crítica, lo que se aconseja es generar respuestas inmediatas ante ataques y protocolos preventivos ante amenazas que pueden resultar comunes.

Autora de la reseña

Viviana Pilar Fuquen Flautero. Ingeniera Industrial, Corporación Universitaria del Meta, Colombia. Especialista en Administración en Seguridad y Salud en el Trabajo, Corporación Universitaria del Meta, Colombia. Técnica en Asistencia, Análisis y Producción de Información Administrativa con énfasis Contable del CENACAP, Colombia. Técnica profesional en Planificación para la Creación y Gestión de Empresas, Servicio Nacional de Aprendizaje, Colombia.

ORCID: https://orcid.org/0000-0002-0714-7895

Contacto: viviana.fuquen@academia.unimeta.edu.co

Referencias

Villagra R., Díaz H., Leiva R., Arteaga M., Marowski C., y Polloni M. (2018). *La ciberseguridad, sus impactos y desafíos*. Centro de Estudios Estratégicos.