DOI 10.52781/cmm.a051

RESEÑA: The fifth domain: defending our country, our companies and ourselves in the age of cyber threats.

CLARKE, Richard A.; KNAKE, Robert K. **The fifth domain**: defending our country, our companies and ourselves in the age of cyber threats. [S. l.]: Penguin Press, 2020. ISBN - 978- 0525561989.

Resumen: El libro trae una cuestión contemporánea esencial: la definición de los límites de acción, protección y uso del ciberespacio como un quinto dominio operativo, así como las medidas a se adoptar para hacer que este ambiente sea más seguro. Utilizando el término adoptado por el Departamento de Defensa de los Estados Unidos, los autores utilizan la experiencia práctica para indicar una agenda que busca la creación de medios para mejorar la defensa de áreas como la seguridad del Estado, la economía, la democracia y la privacidad.

Palabras Clave: Ciberamenazas Ciberespacio. Ciberseguridad. Defensa.

Abstract: The book faces an essential contemporary issue: the definition of the limits of action, protection and use of cyberspace as a fifth operational domain, as well as in the measures to be taken to make this environment more secure. Using the term adopted by the US Department of Defense, the authors use practical experience to indicate an agenda that aims to create means to improve the defense of areas such as state security, economics, democracy and privacy.

Keywords: Cyber Threats. Cyberspace. Cybersecurity. Defense.

Rafael Gonçalves Mota
Universidade de Fortaleza.
Faculdade Ari de Sá.
Tribunal de Justiça do Estado do Ceará.
Fortaleza, CE, Brasil.
rafaelgmota@yahoo.com.br

Recibido: 23 abr. 2021
Aceptado: 28 abr. 2021

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

El libro trae una cuestión contemporánea esencial: la definición de los límites de acción, protección y uso del ciberespacio como un quinto dominio operativo, así como las medidas a se adoptar para hacer que este ambiente sea más seguro. Utilizando el término adoptado por el Departamento de Defensa de los Estados Unidos, los autores utilizan la experiencia práctica para indicar una agenda que busca la creación de medios para mejorar la defensa de áreas como la seguridad del Estado, la economía, la democracia y la privacidad.

El trabajo es fundamental no solo para quienes estudian y trabajan con seguridad cibernética, sino para todos los responsables de pensar los temas relacionados con la soberanía nacional, la alta estrategia y las políticas de defensa nacional. Comprender el alcance de las amenazas concretas en el ciberespacio, especialmente dada la inmensa velocidad a la que opera el panorama cibernético, es esencial para guiar a los tomadores de decisiones en el futuro cercano.

La perspectiva básica del libro sostiene que el panorama del ciberespacio es muy distinto de lo que era hace años. Según los autores, la principal ventaja es que las tecnologías actuales permiten reducir los riesgos que plantean las acciones ofensivas de naturaleza cibernética. Es decir, en la medida que de nuevas tecnologías tienen el potencial de crear nuevas amenazas, también proporciona a los Estados Nacionales herramientas virtuales nuevas y eficientes para defender sus intereses y derechos.

Inicialmente, los autores destacan que el ciberespacio tiene una característica distintiva de otros dominios operativos (mar, tierra, aire y espacio), ya que es el único creado por el hombre. Este hecho, por sí solo, ya hace que el ambiente virtual tenga elementos caracterizadores diferenciados, y es necesario adaptarse y comprender la naturaleza de tales amenazas.

En el diagnóstico de los riesgos, no se debe considerar apenas las acciones agresivas llevadas a cabo por agentes estatales y no estatales. Los defectos, fallas e imperfecciones en los *softwares* y el sistema desarrollados nacionalmente – intencionales o no – abren una brecha para que las actividades maliciosas ocurran más fácilmente y potencialmente más perjudiciales. Con esto, Clarke y Knake señalan que la creación de una política de ciberseguridad debe tener en cuenta dichas variables.

Aún tratando con las vulnerabilidades potenciales derivadas de las características del ciberespacio, los autores comentan la decisión del gobierno de Estados Unidos de ampliar la participación de la iniciativa privada en el suministro de medios cibernéticos, especialmente físicos. En 2015, los principales servidores de *internet*, hasta ahora gestionados mediante contrato con el Departamento de Comercio, fueron transferidos a la gestión privada.

Ante esto, existe una responsabilidad compartida entre los sectores público y privado, que va más allá del uso de medios como las "asociaciones público-privadas" y establece esferas claras de acción compartida. Aunque el campo estatal es directamente responsable de áreas como la acción militar, la investigación criminal cibernética y la recopilación de inteligencia, la protección de datos y las redes cibernéticas privadas no son responsabilidad del Estado, y solo puede haber colaboración gubernamental en situaciones extremas o cuando la acción privada falla.

Al reconocer la imposibilidad del Estado de garantizar, por medios propios y directos, la seguridad del ciberespacio, así como la impropiedad de la iniciativa privada para salvaguardar el ambiente cibernético, los autores indican que no hay un camino o decisión fácil. Lo más seguro sería encontrar la solución menos mala, no necesariamente la mejor, ya que ninguna es completamente efectiva o completamente adecuada.

Desde la administración de Barack Obama, Estados Unidos comenzó a dedicarse a la construcción de una política estratégica de seguridad cibernética, con el objetivo de proporcionar no solo a los agentes estatales, sino también a las entidades privadas, un grado de protección más concreto y efectivo para garantizar la acción en el ciberespacio. Un ejemplo de eso es la creación de la *National Strategy for Trusted Identities in Cyberspace (NSTIC)*. La idea es dotar al ambiente virtual de medios de identificación más seguros y, en consecuencia, de atribución de los actos realizados en él.

Uno de los problemas identificados por los autores al abordar el tema cibernético es una mayor dificultad para imponer una cultura de seguridad unificada en el ambiente privado, ya que, a diferencia de las entidades estatales, los individuos y las empresas tienen acciones más dispersas, dentro de sus propias dimensiones de acción.

En cuanto a la cuestión militar, los autores señalan que el objetivo del Pentágono en relación con un dominio operacional tan peculiar con el ciberespacio es buscar el control completo del sistema virtual. Tal objetivo se indica expresamente en un documento con fecha de 2018, que define la estrategia cibernética del Departamento de Defensa.

Siguiendo en el análisis de la acción militar en el ciberespacio, los autores elaboran una pregunta clave: ¿Puede una organización dirigida a la guerra actuar para reducir las tensiones y reducir la probabilidad de conflictos? Clarke y Knake afirman que la contribución militar es fundamental para reducir las tensiones y los riesgos cibernéticos. Sin embargo, esto debe ocurrir junto con una acción diplomática que cree una arquitectura de relaciones internacionales y favorezca el establecimiento de un ambiente con menos conflictos potenciales y concretos.

La dirección señalada por los autores a la esfera de las relaciones internacionales es la creación de un ciberespacio construido sobre el ejemplo del "Espacio Schengen". Considerando la situación hipotética de un acuerdo internacional en esta línea, es posible construir reglas comunes para la administración y protección de datos. De esta manera, la normalización de los estándares de control y gestión del ciberespacio produciría un ambiente aún más seguro para el desempeño de las compañías y empresas, que pueden competir siguiendo reglas comunes.

Avanzando en el análisis, los autores abordan la necesidad de construir mecanismos eficientes para la protección de las democracias en el dominio virtual. Destacan la creciente importancia del ciberespacio en los procesos electorales, tanto para la capacidad de comunicación como para la evolución de la tecnología de virtualización electoral.

Los autores también destacan que el desarrollo y mejora de la inteligencia artificial, especialmente en el campo de la *machine learning* experimentará un aumento significativo en los próximos cinco años, generando habilidades más eficientes de promoción de medios de defensa, excepto que también hubo una mejora de los actos agresivos.

La conclusión del trabajo es que las estrategias, herramientas y políticas de administración y uso del ciberespacio ya son conocidas y el esfuerzo ahora debe ser canalizado por los países para aprovechar las oportunidades y, sobre todo, tomar decisiones racionales para delinear la próxima era del ciberespacio.


ECEME