Resenha de livro

Cyber war: **the next threat to national security and what to do about it**. Por Richard A. Clarke e Robert K. Knake. 2. ed. New York: Ecco, 2012.[1] ISBN-13: 978-0061962240.

Resenhístas:
Gills Lopes (UFPB e UFPE)
gills@gills.com.br.

Carolina Fernanda Jost de Oliveira (UFPB)
carolinaajost@gmail.com.

Sergio G. Caplan (CAEI)
sergio.caplan@gmail.com.

El ex-asesor en Seguridad Internacional de los Estados Unidos de América (EUA), Richard A. Clarke, y el investigador sobre guerra cibernética del *Council on Foreign Relations*, Robert K. Knake, lanzaron la primera edicion en el mes de abril del 2010. Desde entonces, se ha vuelto el libro de cabecera de muchos *policy makers* y oficiales militares.

El argumento central del libro gira en torno a las potenciales consecuencias que una guerra cibernética (*cyber war*) podría generarle a un Estado, como los EUA, por ejemplo, por ser altamente dependiente de sistemas físicos y lógicos basados en redes. En ese sentido, las infraestructuras críticas, como los sistemas de redes clave para la supervivencia de la sociedad moderna (redes de trenes, gas envasado, energia eléctrica, el sistema financeiro etc.), son tenidas en cuenta como los principales blancos de un potencial ataque cibernético. Por consiguiente, el Estado debe repensar el papel de sus Fuerzas Armadas para enfrentar mejor este nuevo fenómeno.

La obra se divide en ocho capítulos. En esta segunda edición – abril de 2012 –, se añadió un apéndice sobre la intervención de los EUA y de Israel en el intento de sabotear el programa nuclear iraní mediante la utilización de un arma cibernética: un *worm* que conoció como Stuxnet. La inclusión de este *case* en la segunda edición no es menor: además de ser reciente – junio de 2010 –, se puede observar como este evento incluye todos los elementos contenidos en aquello que los autores consideran como *cyber war*.

En el inicio del libro, Clarke y Knake proporcionan un panorama general de lo que se tratará en cada uno de los capítulos para comenzar a abordar la temática central a partir de algunas reflexiones acerca de las iniciativas estadounidenses para desarrollar estrategias nucleares de guerra en las décadas de 1950 y 1960, que hubiesen sido usadas en ataques

[1] Este documento es una versión modificada y traducida de la versión en portugués de: LOPES, Gills; OLIVEIRA, C. F. J. CYBER WAR. **Revista da Escola de Guerra Naval**, 19: 239-42, 2013.

contra Europa y Asia. Con el pasar de los años, el desarrollo de las nuevas teconolgías llevó a la producción de nuevos tipos de armas, requiriendo, por consiguiente, nuevas estrategias. Así, el foco del libro radica en que la creación de este tipo de armas estaria creando un nuevo ambiente para llevar a cabo diferentes conflictos: el ciberespacio. En ese contexto y con la necesidad de diseñar nuevas estrategias, los EUA crearon una organización militar específica, el *United States Cyber Command* (USCYBERCOM). Debido a que la mayor parte de los aspectos que atañen al tema de la guerra cibernética se desarrollan de forma confidencial, el principal propósito de los autores es estimular la apertura de análisis y discusiones públicas acerca del tema, antes de que estalle un conflicto de ese tipo a larga escala.

Los autores describen una serie de ataques – tales como la segunda guerra de los EUA contra Iraq y el ataque de Israel contra Siria – para demostrar los posibles usos de la guerra cibernética como forma de apoyo a los ataques convencionales. En ese caso, el término "guerra cibernética" se refiere a acciones de una nación para invadir computadoras y redes principales de otras naciones, provocándoles daño. Por otro lado, la descripcion de episodios – como hacen com los ejemplos de Estonia, Georgia y Corea del Sur– permite percibir que no sólo los EUA invierten en nuevas alternativas de intervención vinculadas al ciberespacio, sino que otros países ya han identificado también las ventajas de este tipo de estrategia. Además, los incidentes mencionados anteriormente pusieron en alerta a la comunidad internacional, involucrando también a otros actores en este nuevo escenario, como a las organizaciones del calibre de la Organización del Tratado del Atlántico Norte (OTAN), que posee un centro de defensa cibernética propio.

Por medio de la explicación de cómo se creó el USCYBERCOM, se identificaron también algunos factores que estarían involucrados en el propio control del ciberespacio. Se relatan también las funciones y habilidades de los llamados guerreros cibernéticos (*cyber warriors*). Otro aspecto, abordado en el primer capítulo, es el de las estrategias de los EUA para actuar en el ciberespacio, destacando también posibles vulnerabilidades y potenciales enemigos, destacando el ejemplo de China, aunque en realidad no constituya la mayor amenaza para ellos en la actualidad.

Luego, el autor explica como el ciberespacio debe comprenderse de manera estratégica ya que, solo así es posible entender también de qué manera puede ser utilizado para las intervenciones entendidas como guerra cibernética. Ese espacio no está restringido a Internet; ese es apenas el medio por el cual los ataques se podrían manifestar. Existe un fuerte énfasis en la vulnerabilidad de la propia Internet, que debe estar presente en el cálculo de cualquier Estado que pretenda desarrollar sus capacidades cibernéticas. Es por eso que en ese punto, se

percibe la preocupación en discutir el desarrollo de la defensa cibernética en los EUA. Teniendo en cuenta también que los países como China, tienen mayores capacidades en ese área. Anteriormente, esa necesidad no era tan latente ya que no había otras naciones con intenciones de desarrollar capacidades cibernéticas. Hoy, el escenario es completamente diferente.

Países que demuestran mayor capacidad cibernética, o sea, que poseen la mayor parte de su infraestructura en la red, como es el caso de los EUA, resultan ser más vulnerables en un contexto de guerra cibernética. Los países considerados "enemigos" de los EUA tienen capacidades cibernéticas restringidas a la red privada, por lo cual se encuentran menos expuestos a un eventual ataque. El espionaje cibernético es el elemento fundamental de la guerra cibernética, no siendo posible distinguir una de la otra; ambas poseen las mismas características, principalmente en lo que respecta a las relaciones costo-beneficio, ya que, con ese criterio, las dos tienden a ser más ventajosas que sus versiones convencionales, es decir, no existen riesgos potenciales de muerte y son menos costosas.

Si tenemos en cuenta que la guerra cibernética se configura como una posibilidad de intervención político-estratégica más eficiente, habrá más posibilidades de que los daños provocados sean menores a comparación com las armas convencionales. Además de eso, será también más difícil de identificar/controlar el origen de los ataques. Por tantas ventajas, las actividades que se suceden en el ciberespacio atraen el interés de los Estados, con el objetivo de utilizarlas como instrumentos de política exterior. Asimismo, llama la atención de los delincuentes y los terroristas que se desarrollan en este ambiente y que pueden iniciar ataques, sin necesariamente estar vinculados a actores estatales y sus intereses nacionales, haciéndolo por el bien de sus propios objetivos, que en la mayoría de los casos no coinciden con aquellos de los Estados.

Em resumen, la obra, además de situar el concepto estratégico-militar de la guerra cibernética y sus impactos en la sociedad y para el brazo armado del Estado, busca también ampliar la discusión pública sobre la defensa cibernética, sobre todo en los EUA, ya que ella comienza y termina de forma gubernamental. Eso contrasta, por ejemplo, con el caso brasileño, que desde el lanzamiento de su Estrategia Nacional de Defensa, en 2008, viene incentivando, cada vez más, debates civiles y militares sobre uno de los tres sectores estratégicos para el desarrollo nacional: el cibernético. En ese sentido, *Cyber war* pasa a ser una obra clave para entender los desafios y las implicancias que este ambiente engendra para el pensamiento y las acciones militares en el Siglo XXI.