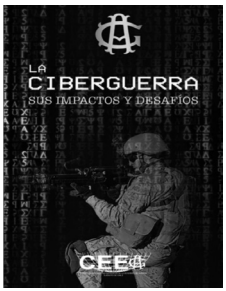
Revista Ensayos Militares
vol. 4 - nº 2 - 2018, pp. 89-91

ISSN 0719-6334 / versión impresa
ISSN 0719-6989 / versión en línea



La ciberguerra. Sus impactos y desafíos

Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile
Santiago: CEEAG, 2018, 168 páginas.
ISBN: 978-956-7734-08-5

Juan Ignacio Brito
Decano Facultad de Comunicación – Universidad de los Andes (Chile)
Email: jbrito@uandes.cl

Un nuevo frente de batalla

La revolución digital es producto del surgimiento de tecnologías de la información que han incrementado exponencialmente la capacidad de almacenamiento, distribución y procesamiento de datos. El impacto es global, porque tiene la capacidad de llegar a todos los rincones del planeta, instantáneo y multidimensional, en tanto afecta a diferentes actividades humanas en diversos ámbitos casi en tiempo real. La generación de cambios relevantes en todo el espectro de dimensiones viene dada por el carácter disruptivo que posee la innovación digital. Clayton Christensen, profesor de la Universidad de Harvard, ha descrito que las nuevas tecnologías de la información amenazan el *statu quo* mediante la aparición de innovadores que inicialmente ocupan lugares secundarios, pero que, gracias a su flexibilidad y capacidad para generar y aplicar conocimiento, terminan desplazando a los actores establecidos[1].

Como no podía ser de otra forma, los Estados han aprovechado el potencial disruptivo de las nuevas tecnologías para la defensa nacional. El avance científico-tecnológico ha

[1] Bower, Joseph L. y Christensen, Clayton M., "Disruptive technologies: catching the wave", en *Harvard Business Review*, enero-febrero 1995. Disponible en https://hbr.org/1995/01/disruptive-technologies-catching-the-wave.

sido una fuente de innovación para el combate, y así como, por ejemplo, pioneros como Giulio Dohuet comprendieron a principios del siglo XX la potencialidad bélica del aeroplano[2], hoy resultan evidentes las consecuencias que involucra el uso de las tecnologías digitales para lo que se ha denominado la ciberguerra, que no es otra cosa que el conflicto bélico en el teatro virtual conocido como ciberespacio.

Por esta razón, resulta muy oportuna la publicación del volumen colectivo *La ciberguerra. Sus impactos y desafíos*, por parte del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. El libro se aboca en primer lugar a definir el concepto en cuestión, a clasificar sus objetivos y a distinguir sus diferentes niveles, desde el individual al sistémico. Al tener la capacidad de generar daños concretos no solo a infraestructura física, sino también a servicios y al almacenamiento virtual de datos, es clave estudiar cuál es la infraestructura crítica que podría verse afectada por una ofensiva digital hostil, aspecto que es abordado por varios autores en el volumen y que reviste especial importancia por las desastrosas consecuencias que puede revestir un daño a la capacidad informática para los Estados, empresas y toda clase de sistemas crecientemente interconectados e interdependientes. La capacidad para generar caos y afectar la toma de decisiones de una ciberofensiva es enorme e involucra asimismo aspectos legales vinculados al derecho internacional público que también son analizados en el volumen.

Aunque parezca que la ciberguerra es un asunto más propio de la ciencia ficción que de nuestra realidad cotidiana, lo cierto es que ella ya se encuentra entre nosotros. En 2015, por ejemplo, *hackers* robaron los datos de 21 millones de ciudadanos norteamericanos luego de que lograran vulnerar los servidores de la Oficina de Administración de Personal (OPM) del gobierno federal de Estados Unidos. Legisladores y funcionarios norteamericanos afirmaron entonces que la mano del gobierno de China se encontraba detrás del ciberataque, aunque Beijing negó tener alguna responsabilidad en el mismo. Meses después de ocurrida la intrusión, el presidente Barack Obama señaló, tras reunirse en la Casa Blanca con su similar chino, Xi Jinping, que ambos países habían acordado evitar el ciberespionaje mutuo en materias comerciales[3], en lo que ha sido lla-

[2] Dohuet, Giulio, *The command of the air* (Nueva York: Coward-McCann, 1942).

[3] Comunicado de la Casa Blanca, 25 de septiembre de 2015. Disponible en https://

mado la "tregua del hackeo" entre las dos superpotencias y un ejemplo de "diplomacia digital" que, sin embargo, no ha evitado que el ciberespionaje siga registrándose[4].

Es que la dimensión bélica de la revolución digital resulta ineludible para cualquier Estado. La dificultad no solo consiste en tener personal técnicamente preparado para hacer frente a las amenazas posibles, sino también en realizar cuantiosas inversiones para mantenerse al día y con capacidad disuasiva en momentos en que la velocidad de procesamiento de la información se incrementa de manera constante y los cambios están a la orden del día. Sin ir más lejos, según el diario The Wall Street Journal, la próxima adopción del estándar 5G "podría darles a las agencias nacionales de inteligencia y a las fuerzas armadas una ventaja para espiar o para intervenir las redes de los países rivales". Al mismo tiempo, el auge de la economía *blockchain*, con la descentralización de la información y el cambio de paradigma que ella involucra en desmedro del *Big Data*[5], supone también un desafío para la manera en que se organiza un ciberespacio que a ratos parece caótico, pero que constituye el escenario ineludible de la ciberguerra y, por tanto, debe ser comprendido y vigilado.

En sus reflexiones finales, *La ciberguerra. Sus impactos y desafíos* establece con acierto que "la tendencia futura de la ciberguerra va en escalada" y por ello propone la generación de nuevo conocimiento estratégico para lidiar con una amenaza cada vez más palpable que debe ser enfrentada en primer lugar con capacidad disuasiva y, eventualmente, por medio del combate en el ciberespacio. Se trata, sin duda, de consejo que debe ser escuchado.

obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

4 Ver Greenberg, Andy, "China tests the limits of its US hacking truce", en Wired, 31 de octubre de 2017. Disponible en https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/

5 Ver Gilder, George, *Life after Google. The fall of big data and the rise of the blockchain economy* (Nueva York: Regnery, 2018).