Revista Ensayos Militares
vol. 4 - nº 2 - 2018, pp. 47-57

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

Robots, ciberguerra y militarización del espacio

Robots, Cyber Warfare and Weaponization of Space

Javier Jordán Enamorado*
Profesor titular de Ciencia Política en la Universidad de Granada

Josep Baqués Quesada**
Profesor de Ciencia Política en la Universidad de Barcelona

Resumen: Este artículo, al tiempo que se refiere a la amplitud de objetivos, facilidad para realizar ataques sorpresa y a la dificultad de atribución de la Ciberguerra, señala que esta, progresivamente, añadirá mayor complejidad a los conflictos internacionales y a la gestión de la crisis. Resalta que la Ciberguerra, para ser eficaz en términos políticos y militares, debe estar respaldada por fuerzas armadas "físicas" que puedan medirse con las de su oponente de manera exitosa. También, destaca que el país que posea las mejores capacidades de ataque de precisión a larga distancia y de sistemas de guerra electrónica más sofisticados será capaz de neutralizar los sistemas de mando y control adversarios y de obtener la superioridad de la información.

Palabras claves: Ciberguerra – Anonimato – Capacidades espaciales – Satélites – Capacidades antisatélites

Abstract: This article analyzes current challenges that the Cyber Warfare deal with. In this regards, it is identified that Cyber War must face to a wide range of objectives, however, it offers the facility to perform surprise attacks; therefore, it is considered that international conflicts will increase in complexity. Furthermore, it is emphasized that in order to be effective in political and military contexts, Cyber Warfare should be supported by actual armed forces that confront to their opponent in the battlefield. Finally, it is noticed that the country with the best long-range precision attack capabilities and electronic war systems, will be able to neutralize the command and control adversary systems, and to achieve information superiority.

Key words: Cyber Warfare – Anonymous – Space Capabilities – Satellites – Anti Satellite Capabilities

Fecha de recepción: 4 de septiembre de 2018
Fecha de aceptación y versión final: 10 de octubre de 2018

---

* Javier Jordán es profesor titular de Ciencia Política en la Universidad de Granada y director del máster en Estudios Estratégicos y Seguridad Internacional de dicha Universidad. Ha sido investigador invitado en el Centro de Estudios Internacionales de la Universidad de Oxford, en el Instituto Europeo de la London School of Economics, en el Instituto de Política Internacional del King's College of London, y en el Departamento de Sociología de la Universidad Hebrea de Jerusalén. Además, es miembro del Grupo de Estudios en Seguridad Internacional (GESI) de la Universidad de Granada. Contacto: jjordan@ugr.es

** Josep Baqués es profesor de Ciencia Política en la Universidad de Barcelona. También ha sido profesor visitante en las Universidades de Lyon II y Pablo de Olavide (Sevilla), y profesor invitado en la Universidad de Granada. Asimismo, es miembro del Grupo de Estudios en Seguridad Internacional (GESI) de dicha Universidad. Contacto: jbaquesq@ub.edu

Presentación

En primer lugar, deseo agradecer la confianza que Javier Jordán y Josep Baqués han depositado en mi persona, al momento de confiarme la tarea de presentar su artículo "Robots, ciberguerra y militarización del espacio", el que es parte del libro *Guerra de Drones. Política, tecnología y cambio social en los nuevos conflictos* que fue publicado por ambos el 2014.

En el artículo, Jordán y Baqués, profesores de la Universidad de Granada y de la Universidad de Barcelona, respectivamente, en primer lugar, abordan las complejidades de la ciberguerra derivadas de sus atributos extraordinarios para realizar ataques sorpresivos sobre blancos estratégicos, manteniéndose el anonimato y dificultando la atribución de dichas acciones. Posteriormente, sin perder la relación con la ciberguerra, se refieren a los sistemas antisatélite en tanto estos permiten perturbar o neutralizar el funcionamiento de los sistemas satelitales del adversario, afectando los sistemas de mando y control y la obtención y entrega oportuna de información.

Respecto de la ciberguerra, producto de los hallazgos logrados por ambos autores, el artículo proporciona al lector sendos ejemplos de ciberataques, los que permiten comprender y dimensionar sus efectos estratégicos y políticos, quedando en evidencia la importancia de poseer capacidades de ciberguerra tanto ofensivas como defensivas para obtener la superioridad en la lucha por el mando y control y por la información.

Algo similar ocurre en lo referido al desarrollo de la capacidad antisatélite, ya que en el artículo se evidencian fundamentos convincentes para entender que ello no es ciencia-ficción sino que, por el contrario, corresponde a una realidad en la que se han involucrado Rusia, China, Estados Unidos y Japón, entre otros. Se suma a lo anterior, el comentario de Jordán y Baqués cuando expresan que los sistemas antisatélite constituyen una amenaza, aun cuando en el caso de Estados Unidos ella sería muy reducida.

Ante la imperiosa necesidad de conseguir la victoria con el mínimo de costo humano, material y financiero, este artículo proporciona antecedentes que conducen a reflexionar positivamente respecto de que la ciberguerra contribuiría a la práctica de la aproximación indirecta al objetivo y, simultáneamente, a la necesaria economía de los recursos citada anteriormente.

Por otra parte, la recomendación referida a que la ciberguerra debe contar con el apoyo de fuerzas armadas "físicas" es coherente con lo que se expresa en la doctrina de diversos países, porque, junto con referirse a lo mismo, también señalan que las operaciones de ciberguerra consideran la ejecución

de acciones mediante fuerzas convencionales. Esto también es coherente con quienes han asumido la disuasión como estrategia defensiva, debido a que la ciberguerra contribuye a conseguir una disuasión que sea creíble por los potenciales adversarios.

Este artículo contribuye a la generación de políticas y estrategias de seguridad y de defensa de los Estados y, simultáneamente, es un aporte para el desarrollo de la cultura, también de seguridad y defensa, que debería poseer la población de cualquier Estado. Es por esto y mucho más que agradecemos a Javier Jordán y a Josep Baqués el habernos autorizado a publicarlo en nuestra *Revista Ensayos Militares*, volumen IV, Nº 2.

General de División (retirado) Mario Arteaga Velásquez
Doctor en Relaciones Internacionales
por la Universidad Complutense de Madrid

Robots, ciberguerra y militarización del espacio

Hace veinte años el título de este epígrafe sonaría a ciencia ficción. Ahora, sin embargo, se refiere a hechos reales y estrechamente vinculados entre sí. Comencemos por la relación entre ciberguerra y robótica militar.

Richard A. Clarke y Robet K. Knake (2011) definen la ciberguerra como "cualquier penetración no autorizada por parte de, en nombre de, o en apoyo a, un gobierno en los ordenadores o las redes de otra nación, en la que el propósito sea añadir, alterar, falsificar información, causar daños o perturbar al adecuado funcionamiento de, un ordenador, un dispositivo de red o los objetos controlados por el sistema informático". Pero, en realidad, esta definición encaja mejor con la de ciberataque, pues tal como está expresada puede referirse a una acción puntual. Nos parece más completa la conceptualización de Adam P. Liff (2012: 405-408), que la entiende como "una situación de conflicto entre dos o más actores políticos, caracterizada por la ejecución de ataques deliberados, hostiles y dañinos contra redes de ordenadores en la infraestructura crítica civil o militar de un adversario con intención coercitiva y orientada a la obtención de concesiones políticas; o como una medida de fuerza bruta contra las redes militares o civiles con el fin de reducir la capacidad del adversario para defenderse o para llevar a cabo represalias semejantes o mediante fuerzas convencionales, así como contra

objetivos militares o civiles con objeto de afectar a un actor por motivos estratégicos". Con el fin de clarificar su definición, Liff señala lo que no sería ciberguerra: ataques físicos contra redes de ordenadores, distribución de propaganda o "guerra psicológica" por medio de internet, ciberespionaje (aunque normalmente sea un paso previo de una acción de ciberguerra), y ataques informáticos que carezcan de una finalidad política o militar directa (lo que excluiría la cibercriminalidad).

Sobresalen algunos ejemplos en la breve historia de esta dimensión del conflicto. Uno de ellos fue el enfrentamiento entre Rusia y Georgia en el verano de 2008. Rusia llevó a cabo ataques distribuidos de denegación de servicios que bloquearon el acceso *web* a los medios de comunicación locales y a las instituciones gubernamentales, así como a los sitios *web* de la CNN y de la BBC, para dificultar que la población georgiana se informarse acerca de la marcha de la guerra. Los ataques también afectaron a los *routers* que comunican Georgia con el exterior, impidiendo que el tráfico con destino exterior pudiera salir. Y también se cortó la comunicación con los bancos extranjeros fingiendo un ataque proveniente de Georgia (Markoff, 2008). Otro caso conocido es el *malware* avanzado "Stuxnet" que en 2009 dañó al complejo iraní de Natanz, destruyendo aproximadamente un millar de centrifugadoras. Se sospecha que el Stuxnet formó parte de la operación "Juegos Olímpicos" desarrollada por Estados Unidos e Israel para retrasar con acciones de ciberguerra el programa nuclear de Irán. A diferencia de otro tipo de *malware,* el Stuxnet además de afectar al funcionamiento de los sistemas informáticos, generaba instrucciones para destruir la maquinaria controlada por dichos sistemas (Sanger, 2012).

Por su peculiar naturaleza las capacidades de ciberguerra poseen ciertos atributos que progresivamente añadirán mayor complejidad a la gestión de las crisis y conflictos internacionales:

a) *Amplitud de objetivos potenciales, incluidos los de carácter militar*. La lista de blancos, además de gigantesca, incluye bienes esenciales para el funcionamiento de un país: desde su red eléctrica, al sistema financiero, pasando por las cadenas de suministros. Eso en el sector civil. En el militar, la adaptación del ejército norteamericano al modelo *Network Centric Warfare* (NCW) constituye un enorme multiplicador de fuerza pero, al mismo tiempo, un peligroso punto débil si el adversario puede explotar las vulnerabilidades cibernéticas (Gordo, 2012).

Conscientes de ello, China y Rusia llevan años invirtiendo en ciberguerra con objeto de reducir la ventaja de las potentes fuerzas convencionales de

Estados Unidos. El Ejército de Liberación Popular de la República China sabe que las fuerzas armadas norteamericanas se sostienen sobre los pilares del sistema logístico y de la infraestructura de C4ISR. De modo que una eventual neutralización de ambos con ciberarmas podría retrasar la participación de Washington en un conflicto o degradar seriamente sus capacidades militares (Krekel, Adams & Bakos, 2012: 8-9). Los resultados serían más eficaces que los que se alcanzarían tratando de destruir convencionalmente los sistemas de armas integrados en la red.

La idea en sí misma no es original. Si la Luftwaffe hubiera concentrado sus ataques sobre los radares y centros de mandos que componían el sistema de defensa aéreo integrado británico, en lugar de bombardear los aeródromos y las fábricas de aviones (y más tarde Londres y otros núcleos urbanos) posiblemente Alemania habría ganado la Batalla de Inglaterra. La novedad en el caso de la ciberguerra es que se trata de ataques "no cinéticos" (sin emplear proyectiles u otras armas similares: un eufemismo anglosajón) que impiden el funcionamiento de la red y que en términos prácticos disminuyen severamente la efectividad de las fuerzas armadas que se basan en ellas.

Clarke y Knake (2011: 82) ponen como ejemplo una guía, escrita por dos oficiales de la fuerza aérea china, para interferir los *data link* de los grupos de combate de portaviones norteamericanos. Obviamente, un ciberataque que lograse tal objetivo no anularía por completo la operatividad del portaviones y de los buques que le acompañan, pero sí que incrementarían su vulnerabilidad frente a las capacidades de denegación de área chinas: misiles balísticos, submarinos diésel y aviones de combate equipados con misiles antibuque.

En septiembre de 2007 Israel demostró cómo un ciberataque puede mermar las capacidades militares de un oponente. Antes de bombardear el reactor nuclear que estaba fabricando el régimen sirio, insertaron un *malware* en el sistema de defensa aéreo enemigo que permitió que los F-15 y F-16 israelíes que se adentraron en el país por la frontera turca no apareciesen en las pantallas de los operadores de radar (Clarke y Knake, 2011: 22).

Si trasladamos las posibilidades que ofrece la ciberguerra al ámbito de los robots, los retos que se plantean resultan evidentes. Desde que su control operativo se interrumpa y se vuelvan "autistas", a que sean dañados a distancia obedeciendo órdenes autodestructivas (como logró hacer el Stuxnet en las centrifugadoras de Natanz), pasando por el peor de los escenarios: que se conviertan en máquinas de guerra "renegadas" que ataquen a sus antiguos dueños.

b) *Irrelevancia de la geografía y facilidad para realizar ataques sorpresa*. Conforme se perfeccionen los instrumentos de ciberguerra será factible que un país con superioridad en esta materia dañe los centros de mando y los escalones logísticos de retaguardia del adversario, aun sin disponer de medios de proyección de fuerzas convencionales (Torres, 2011). La rapidez con que se transmiten los comandos también volverá tentadora la opción de atacar primero, en especial cuanto más mayor sea la dependencia del adversario en los sistemas informáticos. Circunstancia que se incrementará todavía más conforme vaya aumentando el protagonismo de los robots. Por añadidura, jugará a favor del ataque sorpresa el temor a perder los instrumentos de ciberrepresalia tras el primer golpe del enemigo.

c) *Anonimato y dificultad de atribución*. Existen diversos medios para ocultar el origen de un ciberataque. Tanto en lo que respecta a la composición del código del *malware* como al ordenador desde el que se lanza la acción, ya que se pueden utilizar con ese fin ordenadores infectados en países neutrales. El anonimato puede hacer más atrevido al agresor. Y en un contexto de fuerzas armadas cada vez más dependientes de los sistemas no tripulados, eso podría traducirse en un mayor número de incidentes entre las fuerzas de países antagonistas. Los desafíos y enfrentamientos aparentemente controlados suelen acaecer en el transcurso de misiones de espionaje (abril 2001 un caza chino colisionó con un EP-3 Orion norteamericano al que hostigaba), o durante patrullas o maniobras en áreas geográficas disputadas (en marzo de 2010 un submarino norcoreano hundió una corbeta de Corea del Sur, mientras esta realizaba un ejercicio cerca de la frontera, aunque en aguas territoriales propias). Al mismo tiempo, el anonimato también puede hacer menos comprometedora la participación directa de unidades de ciberguerra en conflictos armados por delegación (*proxy wars*), donde una potencia asista a otro gobierno o a un actor no estatal –por ejemplo, un grupo insurgente– en su lucha contra un adversario común.

Una advertencia importante. Los tres puntos que acabamos de ver son características generales sobre el papel. La eficacia real de las acciones de ciberguerra está todavía por demostrarse en el contexto de un conflicto armado. Y a ello se añade el bucle de medidas y contramedidas propio de la tecnología militar. Los ataques de denegación de servicios contra sitios *web* gubernamentales son una minucia comparado con una ciberofensiva a gran escala contra la infraestructura militar de un país avanzado. Para ello son necesarias inversiones en recursos humanos, materiales y organizativos que en la práctica escapan a la mayor parte de los actores estatales y no

estatales. Los esfuerzos de China y Rusia por mejorar sus capacidades de ciberguerra encuentran un paralelo en las actividades del USCYBERCOM: el mando militar de Estados Unidos que centraliza las operaciones de ciberguerra y que, además de tener como responsabilidad la protección de las redes militares norteamericanas, también está desarrollando capacidades ofensivas de ciberguerra.

Por otra parte, para que la ciberguerra sea eficaz en términos militares y políticos debe estar respaldada por unas fuerzas armadas "físicas" que puedan medirse con las de su oponente. No es probable que las capacidades de ciberguerra logren alterar sustancialmente el equilibrio de fuerzas convencionales; y aunque excepcionalmente lo hicieran, desde el punto de vista político sería muy arriesgado jugarse a una sola carta el desenlace del enfrentamiento contra una potencia militar muy superior. El secreto en la ciberguerra se aplica en ambas direcciones. Hasta que no pruebe las ciberarmas contra el enemigo, el atacante no conocerá con certeza el poder destructor real de aquellas y su capacidad para sortear las ciberdefensas del adversario. La confianza excesiva en un "Pearl Harbour cibernético" puede darse de bruces con que el enemigo le estaba esperando o que los daños infligidos son insuficientes. Lo que quizás sí consiga la incógnita sobre la eficacia de la ciberguerra entre grandes potencias es reducir el riesgo de conflicto –incluso limitado– entre ellas, equilibrando de este modo el peligro de que los robots militares hagan más atractivo el empleo de la fuerza entre países con ejércitos avanzados.

Aunque posee elementos distintivos, la ciberguerra y el desarrollo teórico que la acompaña guarda cierta semejanza con los inicios del poder aéreo. Multitud de objetivos son alcanzables desde el aire, al igual que lo son cada vez más desde el ciberespacio. Es comprensible que la ciberguerra genere al inicio una angustiosa sensación de vulnerabilidad. También es indudable que la inversión en este tipo de capacidades tenderá a intensificarse; y que su relevancia será cada vez mayor en términos ofensivos y defensivos en las operaciones militares que se basen en superioridad de información, en sistemas de redes y, crecientemente, en el empleo de vehículos militares no tripulados. Pero hoy, las evidencias están lejos de poder otorgar a los instrumentos de la ciberguerra el calificativo de "arma absoluta", que Bernard Brodie aplicó a la bomba atómica.

Igual que sucede con la ciberguerra, la enorme dependencia que tienen las fuerzas armadas en los satélites, en especial aquellas inmersas en la actual revolución en los asuntos militares (RMA), explica el interés de Estados Unidos, China y Rusia por dotarse de sistemas que perturben o neutralicen

el funcionamiento de los satélites de un potencial adversario. En caso de lograrlo, uno de los sistemas que se verían más afectados serían los robots militares, en especial los drones que realizan vuelos de larga distancia como el Predator, el Reaper o el Global Hawk.

La voluntad de China por dotarse sistemas antisatélite (ASAT) quedó patente en enero de 2007 cuando un vehículo destructor (*Kinetic Kill Vehicle*, KKV) lanzado por un misil balístico SC-19 Fengyun 1C impactó contra un satélite meteorológico anticuado. El éxito de la prueba demostró la capacidad de China para amenazar satélites que vuelan en baja órbita, lo que comprende a los de comunicaciones, de inteligencia de imágenes y de radar (Fuchter, 2009). Justo tres años más tarde, en enero de 2010, China realizó otro ejercicio disparando un KKV desde un misil HQ-19 (una variante del sistema ruso S-400) pero en este caso en misión antimisil balístico. El gobierno de Pekín también está invirtiendo en el desarrollo de láseres de alta potencia para dañar satélites de observación terrestre y estudia el empleo de otros sistemas de dirección de energía como las armas de microondas de alta potencia, cañones electromagnéticos y sistemas de haces de partículas. En 2006 el director de la Oficina Nacional de Reconocimiento norteamericana confirmó que China había iluminado con un láser uno de sus satélites de inteligencia ese mismo año. En un plano de momento teórico, Pekín también tiene interés por los sistemas de contramedidas electrónicas basados en el espacio para interferir satélites de comunicaciones. En una comparecencia ante el Senado en 2007 el General James E. Cartwright, jefe del Mando Estratégico de Estados Unidos, resumía la estrategia china con las siguientes palabras "han emprendido lo que podríamos llamar un proyecto prolongado, disciplinado y comprehensivo por dotarse de medios contra nuestras capacidades espaciales". Pero Washington no es el único que muestra inquietud, India, Japón y Rusia también se sienten afectados (Tellis, 2007).

Durante la época soviética, Moscú invirtió con éxito desigual en varios sistemas antisatélite, que fueron abandonados tras el fin de la Guerra Fría por problemas económicos. Los avances de China y Estados Unidos en materia ASAT han reavivado el interés de Rusia por la cuestión. En marzo de 2009, el general Vladimir Popovkin, en aquel momento jefe de las Fuerzas Espaciales, afirmó que Rusia también estaba desarrollando armas antisatélite, pero sin ofrecer mayores detalles. En enero del año siguiente, su sucesor en el cargo, el general Oleg Ostapenko insistió en la idea pero de manera igualmente vaga. Al parecer Rusia pretende dotar de capacidades antisatélite a los sistemas de misiles antiaéreos S-400 y S-500, cuyo alcance en la actualidad

se encuentra muy por debajo de la altura a la que orbitan los satélites más cercanos a la superficie terrestre.

En la práctica, la amenaza real que plantean los sistemas ASAT contra la infraestructura espacial norteamericana es muy reducida. Estados Unidos cuenta con un número elevado de satélites. Para comunicaciones dispone de cuatro constelaciones diferentes: Advanced Extremely High Frequency System (AEHF), Defense Satellite Communications System (DSCS), Milstar y Wideband Global SATCOM (WGS). Y los avances tecnológicos incrementan la redundancia. Por ejemplo, un solo satélite del WSG (cuyo primer lanzamiento tuvo lugar en 2007) tiene mayor capacidad de comunicación que todo el sistema DSCS (que se remonta a 1982). La red NAVSTAR de posicionamiento global también es capaz de seguir operando aunque se pierdan algunos de sus satélites; y a todo ello hay que añadir el uso eventual de satélites civiles o de países aliados.

Contra un sistema tan redundante las armas antisatélite (ASAT) de impacto directo son escasamente efectivas por su número reducido y su elevado coste económico. Los sistemas ASAT de energía dirigida ofrecen una mayor versatilidad pero todavía se encuentran en una fase demasiado temprana de desarrollo. Mucho más daño provocaría una cadena de detonaciones nucleares a gran altitud, por encima de los 30 km, como consecuencia del pulso electromagnético y de las radiaciones consiguientes. Sin embargo, un ataque así solo tendría sentido en una situación extrema de guerra total. Los efectos serían generalizados, perjudicando también a los satélites del atacante y a los de países neutrales.

Estados Unidos se encuentra en una posición ventajosa a la hora de competir con China y Rusia en tecnología espacial ofensiva. Al igual que la URSS, Washington desarrolló sistemas ASAT desde fines de la década de 1950. Uno de los ejercicios más conocidos tuvo lugar en septiembre de 1985, cuando un misil ASM-135 lanzado desde un caza F-15C Eagle acertó a un satélite que orbitaba a aproximadamente 550 km de altitud. El programa se canceló poco tiempo después, cuando el fin de la Guerra Fría redujo el interés por ese tipo de armas. En 2008, el año siguiente al primer experimento ASAT chino, un misil RIM-161 Standard SM-3 disparado desde un crucero clase *Ticonderoga* destruyó un satélite de observación terrestre que estaba perdiendo altura progresivamente. La prueba fue un éxito a medias. El satélite se encontraba a una altura inferior a la normal y el misil Standard 3 no es capaz de alcanzar a satélites en su órbita habitual (aunque el sistema se podría potenciar en el futuro). En cualquier caso, el lanzamiento envió

un mensaje disuasorio al gobierno chino, cuya economía y fuerzas armadas dependen también cada vez más de los satélites. Por el momento, los chinos tienen más que perder si llevan la guerra al espacio exterior.

La doctrina norteamericana para neutralizar las capacidades espaciales enemigas se basa en tres líneas de actuación: 1) ataque contra los recursos terrestres del programa espacial adversario (infraestructura de lanzamiento, sistema de mando y control de los satélites, y nodos de comunicación de estos últimos); 2) guerra electrónica para interferir en el enlace entre los satélites adversarios y la recepción en tierra; y 3) ataque directo contra los satélites en el espacio. Esta última opción es la menos atractiva por los problemas de eficacia y eficiencia señalados, y porque la destrucción de satélites generaría una nube de restos y partículas que acabarían dañando a los satélites norteamericanos, o a los de países aliados o neutrales (Sheehan, 2009). En 2011 la NASA vigilaba 20.000 objetos con un tamaño superior a una pelota de tenis que se desplazan a una velocidad de casi 7 km por segundo. Lo que debería ser más que suficiente para desincentivar el empleo de armas ASAT de impacto directo. Su desarrollo se podría interpretar como una medida de disuasión, antes que como un instrumento viable contra fuerzas armadas dependientes de la infraestructura espacial.

Los satélites son un elemento esencial de la red donde se integran los vehículos no tripulados a larga distancia; de modo que la generalización de los drones y de otro tipo de robots militares requerirá inversiones paralelas en sistemas de apoyo espaciales. Sin embargo, por las razones que acabamos de apuntar no creemos que en el corto y medio plazo Estados Unidos, Rusia o China vayan a apostar seriamente por expandir la guerra al espacio para neutralizar indirectamente las fuerzas convencionales enemigas. En el futuro lejano la decisión de hacerlo dependerá del desarrollo de medios ASAT capaces de destruir un alto número de satélites sin añadir más basura alrededor de la tierra. Mientras tanto, la neutralización de los sistemas del adversario seguirá basándose en la destrucción de sus instalaciones terrestres y en la interferencia de las señales.

El país que cuente con mejores capacidades de ataque de precisión a larga distancia y de sistemas de guerra electrónica más sofisticados tendrá ventaja a la hora de neutralizar los sistemas de mando y control adversarios, logrando así la superioridad de la información. Es verdad que en la guerra no hay nada seguro y que una vez que se inicia el conflicto, la fricción puede jugar malas pasadas. Pero lo cierto es que hoy Estados Unidos es el más avanzado en robótica militar, ciberguerra y sistemas ASAT. Las vulnerabilidades de la

tecnología van en ambas direcciones. Pueden ser el talón de Aquiles para las fuerzas norteamericanas pero lo mismo puede decirse para las chinas o rusas en la medida en que ellas también dependan cada vez más de los sistemas asociados a la RMA actual.

Bibliografía

Clarke, Richard A. y Knake, Robet K. (2011). *Guerra en la red. Los nuevos campos de batalla*, Barcelona, Ariel.

Fuchter, Kenny (2009). "China's Military Space Strategy", *Air Power Review*, Vol. 12, Nº 2, pp. 52-75.

Gordo, Fernando (2012). "¿Es la ciberguerra un auténtico desafío a la seguridad y a la defensa", *Fuerzas de Defensa y Seguridad*, Nº 408, pp. 28-32.

Krekel, Bryan; Adams, Patton & Bakos, George (2012). *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Report Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, March 7.

Liff, Adam P. (2012). "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *The Journal of Strategic Studies*, Vol. 35, Nº 3, pp. 401-428.

Markoff, John (2008). "Before the Gunfire, Cyberattacks", *The New York Times*, August 12.

Sanger, David E. (2012). "Obama Order Sped Up Wave of Cyberattacks against Iran", *The New York Times*, June 1.

Sheehan, Michael (2009). "Counterspace Operations and the Evolution of US Military Space Doctrine", *Air Power Review*, Vol. 12, Nº 2, pp. 96-113.

Tellis, Ashley J. (2007). "China's Military Space Strategy", *Survival*, Vol. 49, Nº 3, pp. 41-72.

Torres, Manuel R. (2011). "Los dilemas estratégicos de la ciber-guerra", *Ejército*, Nº 839, pp. 14-19.

