

# AIR & SPACE POWER

JOURNAL  
en ESPAÑOL

Volumen 25, N° 2

SEGUNDO TRIMESTRE 2013



EDICIÓN EN ESPAÑOL  
DE LA REVISTA PROFESIONAL  
DE LA FUERZA AÉREA DE  
LOS ESTADOS UNIDOS

<b>Editorial</b>	<b>2</b>
Discurso del Sr. Comandante en Jefe de la Fuerza Aérea de Chile con Motivo del Centenario de la Aviación Militar Chilena <b>General del Aire Jorge Rojas Ávila</b>	<b>4</b>
100 Años de Aviación Militar en Chile: Desde la Aerostación hasta la Idea de Dotar al Ejército de una Especialidad Aérea <b>Iván Siminic</b>	<b>11</b>
Observaciones sobre la Guerra Aérea en Siria <b>Teniente Coronel S. Edward Boxx, USAF</b>	<b>18</b>
Seguridad de las Computadoras: ¿El Talón de Aquiles de la Fuerza Aérea Electrónica? <b>Teniente Coronel Roger R. Schell, USAF</b>	<b>32</b>
Sun Zi en un Desafío Creativo <b>Comodoro José C. D'Odorico, FAA-Ret.</b>	<b>50</b>
El Factor Australiano en la Estrategia del Pacífico Occidental de los Estados Unidos <b>Liao Kai</b>	<b>64</b>
El Dragón y la Computadora: Por qué el Robo de la Propiedad Intelectual es Compatible con la Doctrina China de la Guerra Cibernética <b>Paulo Shakarian Jana Shakarian Andrew Ruef</b>	<b>75</b>
Reenfoco del Pensamiento de la Guerra Cibernética <b>Mayor Sean C. Butler, USAF</b>	<b>86</b>
<b>Reseña de Libros</b>	<b>96</b>



---

## Editorial

---

Al conmemorar el centenario de la aviación militar chilena, nos unimos complacidos a dicha celebración y evocamos solidariamente los avances y los triunfos que hoy hacen parte de tan ilustre historia y a los cuales hacen referencia el distinguido Comandante de la Fuerza Aérea chilena, General Jorge Rojas Ávila, como también el Sr. Iván Siminic, en sus respectivos artículos que encabezan esta edición de nuestra revista. Desde su inicio en marzo de 1913, la FACH se ha convertido en una de las más respetadas y avanzadas fuerzas aéreas de nuestro continente, destacada por sus adelantos tecnológicos, su valioso apoyo a misiones de asistencia regional durante fenómenos y desastres naturales y sus contribuciones a las Operaciones de Paz mundial de las Naciones Unidas.

La seguridad informática abarca una amplia gama de amenazas y problemas tecnológicos que se configuran en debilidades, que ponen precisamente en peligro la seguridad y explotación hostil de los sistemas de información clasificada de la Fuerza Aérea, debido a la creciente vulnerabilidad de las computadoras y redes informáticas contemporáneas y a la notable ausencia de una política firme y comprometida en materia de seguridad que logre el control adecuado de su uso. Al respecto, el Teniente Coronel Schell en su escrito sobre “Seguridad de las computadoras. ¿El Talón de Aquiles de la Fuerza Aérea Electrónica?”, fija su posición sobre los peligros, daños potenciales, y soluciones a este crítico problema de seguridad informática que confrontamos.

Continuando nuestra reflexión sobre el peligro que representa para las fuerzas militares la vulnerabilidad e inseguridad de computadoras y redes informáticas no protegidas suficientemente contra daños y ataques ilícitos, nos detenemos en la exposición presentada por los esposos Shakarian y el Sr. Ruef, en “El dragón y la computadora: Por qué el robo de la propiedad intelectual es compatible con la doctrina china de la guerra cibernética”, a través de la cual examinan y exponen la doctrina y estrategia cibernética china, basada en el espionaje cibernético y en el robo de la propiedad intelectual tanto civil como militar, mediante la implementación de hackers y organizaciones patrocinadas por el gobierno chino.

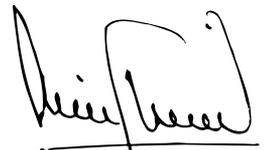
Frente a la crítica situación que vive Siria, derivada de una guerra civil de funestas proporciones, nuestra atención se enfoca en el análisis que en forma objetiva hace el Teniente Coronel Edward Boxx, en su artículo titulado “Observaciones sobre la guerra aérea en Siria”, explorando el uso del poder aéreo durante el desarrollo de esta guerra civil. El autor explica en detalles, el surgimiento de la fuerza aérea siria y sus tácticas, así como también los eventos que condujeron al conflicto actual y puntualiza algunos aspectos que, según su percepción confirman la metodología usada por el régimen de al-Assad en su campaña aérea contra las fuerzas rebeldes, al atacar inicialmente a los civiles con helicópteros y luego con aviones de combate en el desarrollo de una sangrienta y psicológica operación que le ha permitido impedir el avance de los rebeldes y retrasar el colapso del régimen. El Coronel Boxx concluye su exposición con algunos interrogantes que se plantea sobre la falta de participación directa de Estados Unidos y las consecuencias que le podrá acarrear su lamentable ausencia de liderazgo en el conflicto.

La presencia de China en la región del Pacífico Occidental, sumada al panorama estratégico que se vislumbra en los alrededores y más allá del Mar del Sur de China, así como también a las disputas territoriales e implicaciones tanto para los Estados Unidos como para los países regionales constituyen un factor de preocupación. Sr. Liao Kai ofrece una interesante perspectiva en su aporte “El factor australiano en la estrategia del Pacífico Occidental de los Estados Unidos”

conjuntamente con sus conclusiones sobre el efecto nefasto que dichas actividades expansionistas chinas implican para los intereses estratégicos estadounidenses y regionales.

Al hacer referencia al resurgimiento de nuevos conflictos bélicos ahora denominados como *guerra no convencional*, el ilustre analista José D’Odorico, en su artículo “Sun Zi en un desafío creativo”, contrasta los pensamientos y dictados del famoso estratega chino Sun Zi, relacionados con el arte de la guerra y la evolución del pensamiento de la guerra moderna que se caracteriza por conflictos provenientes del *crimen organizado*, el *narcotráfico*, las *guerrillas mercenarias* y las *migraciones invasivas* que podrían poner en riesgo la victoria, como el principal objetivo de la guerra. Al mismo tiempo, el autor hace énfasis en los peligros que afrontan algunas naciones por la carencia de un debido estudio de estos conflictos y la falta de información al pueblo sobre las consecuencias de dichos conflictos.

Finalmente, pese a los esfuerzos sostenidos por introducir avances en materia de informática aplicada al ciberespacio y, al largo camino recorrido por la teoría cibernética militar durante los últimos diez años por lograr su actualización, nos encontramos aún frente a una tendencia natural, un tanto persistente de concebir al ciberespacio como un entorno físico con principios de combate propios de los otros dominios operacionales tradicionales. En su intento por establecer las bases para el desarrollo de una teoría sólida, el Mayor Butler en su artículo “Reenfoco del pensamiento de la guerra cibernética” se propone identificar el núcleo que define las características del ciberespacio, señalando los errores en la utilización de paradigmas ciberespaciales físico-orientados como base para el desarrollo de la doctrina cibernética y propone la necesidad de un enfoque virtual en lo que respecta a su naturaliza y a su capacidad de procesar, intercambiar y almacenar información rápidamente a través de medios automatizados. En este sentido, el autor concluye su exposición con la identificación de algunas de las implicaciones que desafían los intentos existentes por aplicar directamente el poder aéreo tradicional y los principios de guerra al ciberespacio.



Teniente Coronel Luis F. Fuentes, USAF-Retirado  
Editor, *Air & Space Power Journal—Español*



## **Discurso del Sr. Comandante en Jefe de la Fuerza Aérea de Chile con Motivo del Centenario de la Aviación Militar Chilena.**

EL BOSQUE, 07 DE MARZO 2013

**Nota del Editor:** A continuación presentamos el texto del discurso pronunciado por el Sr. General Jorge Rojas Ávila, Comandante en Jefe de la Fuerza Aérea de Chile, con motivo de conmemorarse los 100 años de la Aviación Militar Chilena y de la Escuela de Aviación “Capitán Manuel Ávalos Prado”, el cual ha sido autorizado para ser publicado en nuestra revista por el Departamento Comunicacional de la Fuerza Aérea de Chile.

### **INTRODUCCIÓN**

Me ha correspondido el alto honor de estar comandando la Fuerza Aérea de Chile, en este año 2013 en el que se cumplen dos hitos trascendentes para la aeronáutica nacional y para el país: el Centenario de la Aviación Militar Chilena y el Centenario de la Escuela de Aviación.

Los aviadores del presente hemos querido conmemorar ambos hechos en esta solemne ceremonia, que se ve realizada por la presencia de las más altas autoridades nacionales, de muy apreciados invitados extranjeros y nacionales, de representantes del mundo aeronáutico y de la gran familia aérea.

Les agradecemos profundamente a todos su amable presencia, y en forma muy especial, a S.E. el Presidente de la República, don Sebastián Piñera Echenique, que nos hace el honor de presidir esta ceremonia; los saludamos con nuestro mayor aprecio y les damos nuestra más cordial bienvenida a esta histórica Base Aérea El Bosque, cuna de la aviación militar chilena.

### **UN SIGLO DE ALTO VUELO PARA CHILE**

Hace poco más de 100 años, el 11 de Febrero de 1913, se creó en este mismo lugar la Escuela de Aeronáutica Militar, con unas frágiles aeronaves, propias de los inicios de la aviación en el mundo. Hoy, ese mismo establecimiento, transformado en la Escuela de Aviación “Capitán Manuel Ávalos Prado”, imparte instrucción de vuelo a sus cadetes en aviones T-35 “PILLÁN” fabricados en Chile y exportados también a otros países.

Hace también 100 años, el 07 de marzo de 1913, en un día como hoy, el Capitán Manuel Avalos Prado realizó en este aeródromo el primer vuelo de un avión militar chileno, pero las reducidas capacidades del avión le permitieron solamente sobrevolar el campo aéreo y sus alrededores. El pasado mes de Octubre, aviones de combate chilenos se trasladaron en vuelo directo y con reabastecimiento en el aire, desde Iquique hasta los Estados Unidos, a más de 6.000 kilómetros de distancia y cruzando el espacio aéreo de siete países.

Estos dos ejemplos, resumen lo que ha sido el desarrollo de la aviación militar en estos cien años, en cielos nacionales y extranjeros; una verdadera epopeya que representa las vivencias y los anhelos de miles de personas y de sus familias; la voluntad de autoridades visionarias que respaldaron a la aviación, y fundamentalmente, los esfuerzos y sacrificios de miles de aviadores que imbuídos de su ideal aéreo, quisieron enfrentar los desafíos, los peligros y la muerte.

Todos los integrantes de la Aviación Militar Chilena, ya sean de la Aviación del Ejército, de la Aviación Naval y de la Fuerza Aérea de Chile; merecen ser recordados con agradecimiento y respeto; y para ello, los aviadores del presente les rendimos hoy nuestro más sentido homenaje.

Quienes dieron origen a la aviación en el país, a comienzos del siglo pasado, intuyeron que en ella estaba la clave que la modernidad nos ofrecía, no solo para la conectividad interna de nuestro territorio, sino también para la de Chile con el resto del mundo. Sin embargo, aquella intuición chocaba con dos obstáculos formidables.

Uno de ellos era la inmensa barrera natural de la Cordillera de los Andes, todo un desafío a vencer para crear accesos al exterior, por la vía aérea. El otro obstáculo, era la insuficiente tecnología disponible, la misma que hacía parecer un sueño la idea de cruzar en vuelo el macizo andino.

Hitos como el cruce de la Cordillera de Los Andes en 1918 por el Teniente Dagoberto Godoy, el doble cruce de la misma, al año siguiente, por el Teniente Armando Cortínez, o el raid Santiago-Río de Janeiro del Capitán Diego Aracena en 1922, mostraron a los chilenos que nuestra geografía podía y debía tener una mejor y más eficaz conectividad, si se desarrollaba en plenitud a la aviación.

La sociedad, las autoridades, nuestros conciudadanos, asumieron este gran desafío y fue así como en estas diez décadas, se forjaron sucesivos caminos alados para la Patria, hasta llegar a conectar plenamente la tricontinentalidad de Chile, en sus dimensiones continental, antártica e insular pacífica y más aún, se abrieron los cielos del mundo para nuestros compatriotas.

Por eso, si hoy nuestra mirada se dirige hacia el pasado, es para agradecer el enorme legado que recibimos generosamente de quienes nos precedieron en los cielos patrios.

No puede menos que admirarse la visión futurista y la convicción del Presidente Ramón Barros Luco y de sus asesores en 1913, quienes apostaron por el futuro de la aviación para Chile, cuando la población nacional recién alcanzaba los 3 millones y había en el país solamente 21 automóviles. No menos loable fue la predisposición del Ejército y luego de la Armada, para incorporar el medio aéreo a sus potenciales bélicos. Esto llevó pronto a una perspectiva más amplia, por cuanto además de la aviación militar, se consideró también el desarrollo de la aviación civil, de la comercial, de una industria aeronáutica propia y el fomento de una conciencia aérea en la población.

Esta concepción se materializó fundamentalmente entre 1926 y 1930, gracias al empuje, la tenacidad y la visión del Comodoro Arturo Merino Benítez, quien logró iniciar la aviación comercial con la creación de la Línea Aeropostal Santiago-Arica, reorganizó el Club Aéreo de Chile y estableció la primera fábrica de aviones, en Los Cerrillos, todo lo anterior, con una creciente acogida ciudadana a la aviación.

## LA FUERZA AÉREA DE LOS CHILENOS

Los logros indicados abrieron el camino hacia un propósito mayor, la creación de un arma aérea independiente, como empezaba a ser realidad en otros países. Fue así como, el 21 de Marzo de 1930, el Gobierno determinó fusionar la Aviación del Ejército con la Aviación Naval, para concentrar en una sola Institución y bajo un solo mando, todo lo concerniente a la aeronáutica militar. Chile se inscribía así entre los cinco primeros países del mundo en contar con una Fuerza Aérea independiente.

De nuestros ancestros militares y navales recibimos no solo sus dotaciones, aviones e instalaciones, sino también un valioso legado de experiencias, valores y tradiciones, que han facilitado siempre el entendimiento y nuestra acción conjunta dentro de la Defensa Nacional.

La Fuerza Aérea asumió la continuación de este vuelo de progreso. Durante décadas, hemos cumplido millones de horas de vuelo, en el territorio continental, antártico e insular de la República, especialmente en aquellos lugares donde solo el avión o el helicóptero pueden conectarlos con el corazón del país, enfrentando climas y geografías consideradas entre las más difíciles del mundo. En 1930, el Comodoro Merino Benítez planteó el gran desafío de utilizar “*el camino de los cielos de Chile*” para unir a los habitantes de sus lugares más extremos o lejanos, y lo hemos logrado plenamente, reforzando en ellos su sentido de pertenencia a nuestra Patria.

Nuestra actividad se ha proyectado también al extranjero, honrando los compromisos de la política exterior de Chile ante la comunidad mundial, especialmente en Operaciones de Paz de Naciones Unidas. Recientemente, con nuestra Unidad de Helicópteros, cumplimos 12.000 horas de vuelo como integrantes de la Misión de las Naciones Unidas para la Estabilización de Haití-MINUSTAH.

Mantenemos nuestro entrenamiento y alistamiento operacional, participando en diversos ejercicios, con Fuerzas Aéreas de avanzado nivel, practicando modalidades de coaliciones aéreas internacionales, que eventualmente pudieran ser empleadas en pro de la paz mundial.

Pero fundamentalmente, nuestra trayectoria representa las vivencias, el esfuerzo, los sueños y la historia de alrededor de 85.000 personas y sus familias. Ellos han sido los oficiales, suboficiales y civiles, que en distintas épocas han integrado esta Institución y que bajo la conducción de 24 Comandantes en Jefe, la han mantenido *volando por y para los chilenos*.

Hoy podemos afirmar con total convicción y orgullo, que el sistema aeronáutico planteado por nuestros antecesores, es una palpable realidad, en su plena madurez, moderno e integrado, que contribuye a la defensa, a la conectividad, y al desarrollo de sus habitantes.

Dentro de este sistema, la Fuerza Aérea ha sido siempre una Institución con un fuerte componente tecnológico, el cual asimila para sí, pero también lo desborda hacia la comunidad nacional, en beneficio de su bienestar y progreso.

Una nueva estructura sistémica, generada en la década de los años ochenta y más adelante una visión política moderna del desarrollo y empleo conjunto de las Fuerzas Armadas, nacida en la década de los noventa, han llevado a que la Fuerza Aérea del presente tenga un rol disuasivo plenamente vigente y reforzado, como un importante pilar de la defensa nacional.

La incorporación de sistemas de armas de cuarta generación, de moderno material de transporte estratégico y de helicópteros, nos dan la capacidad de apoyar efectivamente la política exterior del Estado en situaciones de crisis, de empleo del Poder Militar, o a través de Operaciones de Paz de Naciones Unidas, cuando sea requerido.

Desde otra dimensión, también hemos aportado efectivamente a la integración de los chilenos, especialmente en zonas apartadas y hemos estado junto a ellos para socorrerlos ante desastres naturales o emergencias médicas.

Las rutas que hemos abierto en los cielos nacionales, las hemos prolongado para proyectar al país más allá de sus fronteras terrestres, llegando a cualquier lugar del mundo donde lo dispongan nuestras autoridades y hemos llevado esta idea de conectividad aérea, hacia su prolongación

natural, el espacio exterior, a través de nuestros proyectos satelitales de la serie FASAT, que comenzamos a poner en órbita a partir de los años 90.

El más reciente de ellos, el FASAT CHARLIE, en poco más de un año, operando a 600 kilómetros de altura, entrega imágenes de alta calidad que combinamos con capas fotográficas aéreas para abrir a la comunidad una plataforma de información precisa para proyectos y estudios, como también para apoyar la formulación de políticas públicas sobre el territorio nacional.

No menos importante resulta actualmente, la actividad y el apoyo que tienen la aviación comercial, civil y deportiva, que impulsara tempranamente el Comodoro Merino Benítez. Al día de hoy se encuentran matriculadas más de 1.600 aeronaves civiles, las cuales comparten con las de naturaleza militar una red aeroportuaria de 347 aeródromos y 127 helipuertos, distribuidos entre Arica y la Antártica y los territorios insulares. En ellas se realizan anualmente más de medio millón de operaciones aéreas. Para graficar lo que esto significa, recordemos que en los inicios de la aviación comercial chilena, en 1930, se transportaban 5.200 pasajeros anuales; hoy son más de 15 millones y se mueven por aire, cerca de 320 mil toneladas de carga.

Esta red cuenta con modernas ayudas a la navegación y servicios meteorológicos apoyados en redes satelitales, con un 100% de cobertura radárica, cuya información fluye interconectada y en tiempo real a lo largo del territorio. Todo este sistema es operado por personal altamente calificado y entrenado, cuyos estándares y niveles de exigencia nos convierten en uno de los países más seguros para el vuelo a nivel regional y mundial.

Esta afirmación está avalada por el hecho que la FAA- la Administración Federal de Aviación de los Estados Unidos, considera desde 1991 a nuestro país en Categoría Uno en términos de seguridad operacional, lo que significa que los aviones de Chile pueden acceder y operar libremente en el espacio aéreo estadounidense, lo que es de primordial importancia para las empresas aéreas que realizan el transporte entre ambos países, tanto de pasajeros como de carga.

Por otra parte, Chile se encuentra catalogado desde 1997 entre los diez mejores países del mundo, de acuerdo a las auditorías de seguridad operacional que realiza la Organización de Aeronavegación Civil Internacional – O.A.C.I. A través de esta misma organización de las Naciones Unidas, se le ha entregado a nuestro país la responsabilidad del control y ayuda a la aeronavegación en un *espacio aéreo controlado*, que se superpone sobre una superficie de 31,9 millones de kilómetros cuadrados, siendo uno de los mayores del planeta.

Los límites Oeste y Sur de este Espacio Aéreo Controlado por Chile tienen una especial importancia.

Hacia el Oeste, más allá de 5.000 kilómetros en el Océano Pacífico, nuestro Espacio limita con aquellos asignados a la responsabilidad de Tahití y de Nueva Zelanda, conformando el acceso natural aéreo de Chile hacia la Región de Asia/Pacífico. Hacia el Sur, nuestro Espacio Aéreo Controlado se prolonga hasta el mismo Polo. Esta es una de las razones por las cuales la Fuerza Aérea ha mantenido desde la década de los 80 una constante penetración hacia la profundidad del territorio antártico, estableciendo sub-bases y llegando en varias oportunidades a la zona polar.

El control y apoyo a la aeronavegación que se realiza sobre estos 31.9 millones de kilómetros cuadrados ya mencionados, es una responsabilidad compartida entre la Fuerza Aérea y la Dirección General de Aeronáutica Civil, a través de un trabajo integrado de alta exigencia, que requiere una acabada preparación profesional y un entrenamiento constante, para enfrentar grandes volúmenes de tráfico con precisión y oportunidad, velando por las miles de vidas humanas a bordo de las aeronaves.

De allí entonces que, en lo que se refiere al control del Espacio Aéreo, la Fuerza Aérea y la Dirección General de Aeronáutica Civil constituyen en la práctica dos partes de un mismo todo, afiatado y eficaz, que labora en equipo para otorgar confianza y seguridad a los operadores y a sus pasajeros.

Puede concluirse entonces, que el desafío planteado por las autoridades y los aviadores de los primeros tiempos, ha sido debidamente recogido y desarrollado por las sucesivas generaciones, para hacer de nuestros cielos verdaderos caminos aéreos de progreso y de comunicación.

El desarrollo aeronáutico nacional no solo se expresa en las actividades de vuelo, sino también en otras expresiones que lo proyectan hacia la comunidad, como han sido la creación de la Empresa Nacional de Aeronáutica-ENAER; la realización periódica de la Feria Internacional del Aire y del Espacio-FIDAE y el complejo trabajo que realiza el Servicio Aerofotogramétrico-SAF.

La aviación llega también hacia los ciudadanos en las presentaciones de nuestras Escuadrillas de Alta Acrobacia "HALCONES" y de Paracaidistas "BOINAS AZULES"; en las embajadas culturales de nuestra Banda Sinfónica a lo largo del país y, especialmente, en el estrecho contacto con nuestros compatriotas durante los operativos aeromédicos que realizamos a lo largo del territorio.

Los antecedentes indicados avalan la enorme importancia que tiene para Chile su *espacio aéreo*, como recurso inagotable de crecimiento y de proyección, entendiéndolo como un bien nacional de uso público y un instrumento abierto al progreso nacional.

Para mantener y potenciar su desarrollo, es necesario poner énfasis en factores específicos, como son las tecnologías, los costos, la inversión en infraestructura aeroportuaria, las relaciones económicas entre el sector público y el sector privado, y sobre todo, en la naturaleza mixta de una red aeronáutica civil/militar, que garantiza no solo el desarrollo económico, sino que también la estabilidad y la seguridad de su tráfico aéreo.

## NUESTRA PROFESIÓN

De acuerdo a las actividades que he mencionado, se podrá apreciar que hemos sostenido el ritmo de nuestro quehacer y que mantenemos el alistamiento operacional que nuestra misión nos demanda. Lo hemos hecho porque tenemos la convicción como aviadores, que nuestra profesión es de servicio público. Servir a nuestra Patria, ayudando a mantener una seguridad nacional, a producir una estabilidad que permita a la ciudadanía trabajar y desarrollarse en paz, viene a ser, en último término, la manifestación más concreta y valiosa de nuestra Responsabilidad Social institucional.

La profesión de aviador militar, es una actividad seria, delicada y difícil, que necesita de todas nuestras energías y dedicación. Esto se ha hecho más acuciante en la medida que hemos incorporado tecnologías más complejas. Por ende, la Fuerza Aérea está en una búsqueda permanente de modalidades y contenidos, para crear mejores profesionales y darles la mayor capacitación que requieran para el cumplimiento de sus deberes, sin descuidar su formación de soldados.

Nuestra meta permanente es disponer de una dotación profesional, que funcione como un equipo disciplinado y coordinado. Es fundamental que esta dotación esté cimentada sobre los valores y virtudes del aviador, porque ellos son el pilar y fortaleza de los hombres y mujeres que han elegido servir a la Patria a través de la Fuerza Aérea de Chile.

Por esta razón debe tener un conjunto de valores y virtudes encarnadas en su persona y debe transmitirlos con su propio ejemplo a los demás, en forma especial, a sus subordinados. Este deber moral es especialmente exigible en el caso del Oficial, al cual junto con asignarle su deber, se le entrega valioso capital humano y recursos materiales de alto costo.

La delicada labor de fijar en forma indeleble este conjunto valórico en los Oficiales, es la responsabilidad primordial de la Escuela de Aviación. Continuadora de la primera Escuela de Aeronáutica Militar, que se creara en 1913, ha sido durante sus cien años de vida un verdadero crisol de virtudes que impregnan y distinguen a quienes han pasado por sus centenarias aulas.

A partir de 1942 se iniciaron en ella los cursos de Cadetes de Aviación, condición en la que más de 10.000 jóvenes chilenos han integrado sus filas, algunos continuando la carrera y otros buscando nuevos horizontes en la vida civil. Desde entonces, nuestra Alma Mater ha entregado

84 promociones de Oficiales a la Fuerza Aérea, que la han servido con dedicación, justicia, fortaleza y prudencia, honrando el lema de la Escuela: “COMPOS SUI”, Dueño de Sí mismo, y haciendo patente la formación que recibieron, inspirada en los valores básicos de la Institución: Honor, Lealtad, Cumplimiento del Deber y Excelencia en el Servicio.

Representando el sentir de todos mis camaradas y de todos aquellos que tuvimos la honra de vestir el uniforme de Cadete de Aviación, presento mi saludo más afectuoso a la Escuela de Aviación al cumplir sus 100 años de existencia y formulo sinceros votos porque continúe siempre su vuelo exitoso “con la vista clavada en los cielos”, como dice su himno, rumbo a la superación.

## CONDECORACIÓN

Cumplidos los cien años de estos dos hechos que hoy conmemoramos, hemos querido dejar un sello indeleble de ellos, a través de la Condecoración “CENTENARIO DE LA AVIACIÓN MILITAR CHILENA Y DE LA ESCUELA DE AVIACIÓN” que se entregará por única vez, con este motivo.

La hemos establecido para expresar un reconocimiento material y permanente, hacia aquellas personalidades que dentro de su ámbito de acción, hayan efectuado un aporte significativo a la Aviación Militar Chilena y a la aeronáutica nacional.

A través de esta preseña, los aviadores queremos hacer presente nuestro reconocimiento hacia quienes han vibrado con nuestros logros y nos han ayudado a obtenerlos, estando cerca nuestro con su amistad y apoyo. Es también una forma propicia para reforzar los lazos con todos quienes tienen un lugar especial en nuestros afectos y para demostrarles nuestra consideración y aprecio de una forma especial y tangible.

Tendremos el honor de imponerla, en primer término, en la persona de Su Excelencia el Presidente de la República, don Sebastián Piñera Echenique, en quien hemos encontrado siempre una gran comprensión, empatía y apoyo irrestricto con los diversos temas relativos a la Institución y a la actividad aérea, en sus diversas manifestaciones. Sabemos su interés por nuestra actividad, lo hemos percibido cuando ha volado en nuestras aeronaves a lo largo del territorio, lo hemos apreciado en su contacto llano y directo con nuestras tripulaciones, avalado por su experiencia como piloto y por todo ello, agradecemos profundamente su confianza y soporte.

Esta Condecoración será impuesta hoy también al Estandarte de Combate de la Escuela de Aviación. Este establecimiento, que ha sido durante un siglo un verdadero crisol generoso de aviadores para Chile, lo sigue siendo para hombres y mujeres como estos Cadetes aquí presentes, que buscan en ella alas para la vida y un propósito para sus existencias, a través de la desafiante carrera de Oficial de la Fuerza Aérea de Chile.

Entregaremos también esta Condecoración al Sr. Ministro de Defensa Nacional, don Rodrigo Hinzpeter Kirberg, quien dentro de sus altas funciones, ha tenido una gran preocupación, permanente respaldo y total colaboración respecto del quehacer institucional, su equipamiento y su nivel de alistamiento operacional, dentro de la perspectiva conjunta, que caracteriza la moderna arquitectura de la defensa nacional.

Impondremos esta condecoración a los Sres. Comandantes en Jefe del Ejército y de la Armada, como también al Sr. General Director de Carabineros y al Sr. Director General de Investigaciones, como una forma de renovarles nuestro reconocimiento por su permanente amistad hacia la Fuerza Aérea, reflejada en la confianza, apertura y amplio espíritu de colaboración con que interactuamos día a día y lo hemos hecho a lo largo de nuestra historia.

Queremos rendir también el más sincero y agradecido homenaje a nuestros ancestros, la Aviación del Ejército y la Aviación Naval, que en 1930 se fundieron en un abrazo noble y generoso para darle a Chile el arma aérea que los tiempos señalaban y que el país requería. Hemos invitado especialmente a ambas, para que estén representadas por una sección con su Estandarte de

Combate, al cual prenderemos esta Condecoración, como muestra permanente de reconocimiento, agradecimiento, respeto y hermandad aérea.

Con especial fraternidad y camaradería aérea, impondremos esta Condecoración a los Sres. Comandantes Aéreos titulares de Argentina, Brasil, Canadá, Colombia, España, Paraguay, Perú y Uruguay, que han concurrido a Chile con un mensaje de confraternidad, permanente apoyo y buen entendimiento, que apreciamos en toda su valía y que agradecemos profundamente. Igualmente, se han hecho merecedores a esta Condecoración los Sres. Jefes Aéreos titulares de Alemania, Ecuador, Estados Unidos, Francia, Italia, Reino Unido y Turquía, representados aquí por sus delegaciones, y la cual les será entregada oportunamente en nuestras Embajadas en sus respectivos países.

Hago propicio este momento para saludar particularmente y destacar, la presencia de las delegaciones de las Escuelas Militar y Naval de Chile y de las Escuelas Matrices aéreas de países amigos, que han concurrido a manifestar su adhesión y homenaje con motivo del Centenario de la Aviación Militar y de la Escuela de Aviación.

## CONCLUSIÓN

Quiero finalizar mis palabras recordando, especialmente a estas jóvenes generaciones formadas frente a nosotros, que el progreso de la aeronáutica ha sido y sigue siendo incontenible, y así lo hemos visto en estos cien años, por lo que debemos estar siempre preparados para los avances que vienen. Pero no debemos olvidar por ello, a quienes hicieron posible este progreso, a los miles de hombres y mujeres que en cada época entregaron su aporte personal y a veces sus vidas, por cumplir con su deber y por hacer cada vez más grande a su Patria.

Todos ellos, enfrentaron duros desafíos, algunos materiales, otros de incomprensión, pero todos exigieron lo mejor de sí mismos para potenciar sus fortalezas, suplir sus carencias y cumplir a todo trance con su deber. No fue fácil, especialmente al principio, en un difícil territorio como el nuestro, pero lucharon contra el desierto o las heladas planicies australes, vencieron el calor agobiante o el intenso frío, sostenidos por la convicción de estar forjando nuevos rumbo de progreso para Chile.

Desde aquellos biplanos, con sus cabinas abiertas a las inclemencias del tiempo, hemos llegado a los actuales aviones supersónicos, de sofisticada tecnología. Por lo mismo, debemos recordar con un gran respeto y agradecimiento los nombres de aquellos intrépidos pioneros y a quienes les siguieron, porque ellos plantaron las bases sobre las cuales se yergue esta Fuerza Aérea del siglo XXI, moderna y altamente tecnologizada, pero igualmente aguerrida y pujante, como nuestros precursores.

Sus logros son un ejemplo de vida, que merece todo nuestro agradecimiento y que nos debe servir de inspiración para superarnos cada vez más.

En este día tan especial para la Aviación Militar de Chile y para la Escuela de Aviación, exhorto a mis camaradas de la Fuerza Aérea, hombres y mujeres, jóvenes chilenos, para que unamos nuestras voluntades y redoblemos nuestros esfuerzos para seguir siendo un aporte para Chile y para todos nuestros compatriotas. Junto con agradecer profundamente su trabajo esforzado día a día en nuestras Bases y Unidades, los insto a que sigamos entregando toda nuestra capacidad intelectual y profesional, y nuestro ejemplo personal, para mantener esta Fuerza Aérea sólida, cohesionada, moderna y eficiente, como nuestros conciudadanos esperan de nosotros.

Continuemos afianzando los caminos aéreos de la Patria, porque es ella la que explica nuestro pasado y no concebimos el porvenir sin estar a su pleno y total servicio.

Volemos siempre más rápido, más alto, más lejos, porque allá está el futuro y debemos conquistarlo.

Muchas gracias.

General del Aire Jorge Rojas Ávila  
Comandante en Jefe de la Fuerza Aérea de Chile

# 100 Años de Aviación Militar en Chile

## Desde la Aerostación hasta la Idea de Dotar al Ejército de una Especialidad Aérea

IVÁN SIMINIC

*Las autoridades militares nacionales fueron pioneras en reconocer y dimensionar el papel que jugaría la aviación en los conflictos por venir. En tal sentido, asesoraron convenientemente a la autoridad política chilena de la época y dieron los pasos necesarios para hacer realidad una audaz idea muy poco tiempo después de que la misma tendencia se impusiera en Europa.*

### Llegada de la aerostación

Luego de que a contar de 1783 los Montgolfier ganaran fama con sus globos en Francia, Luis XVI, el mismo monarca parisino que había instado a dichos hermanos para que las pruebas de vuelo de sus aerostatos se hicieran transportando personas, envió en viaje a zonas remotas del globo al navegante y botánico Jean François de Galaup, Conde de la Pérouse (1741-1788) con la misión de completar los descubrimientos científico-biológicos de James Cook en el Pacífico y de establecer -también- vínculos político-estratégicos con sus aliados españoles en las islas Filipinas.

En su viaje, La Pérouse llegó a Chile en 1785, desembarcando en la provincia de Concepción. Dentro de las actividades a realizar se dio la posibilidad de elevar un globo sin tripulantes, hecho que se considera como el primero de su tipo dentro del territorio nacional.

Años después, en el Santiago de 1839 se produjo la visita de un norteamericano que quiso ganar algún dinero mediante la exhibición de algunos globos que pretendió elevar en la Plaza de Armas de la ciudad. Luego de que la primera tentativa fracasara y provocara gran enojo popular, habría sido un joven chileno de nombre desconocido quien se habría asociado con el extranjero para prestarse como pasajero de dichas elevaciones, las que tuvieron éxito comercial durante algunas semanas.

En septiembre de 1857, Luis Vernert, otro aeronauta francés, visitó la capital y también logró hacer algunos ascensos.

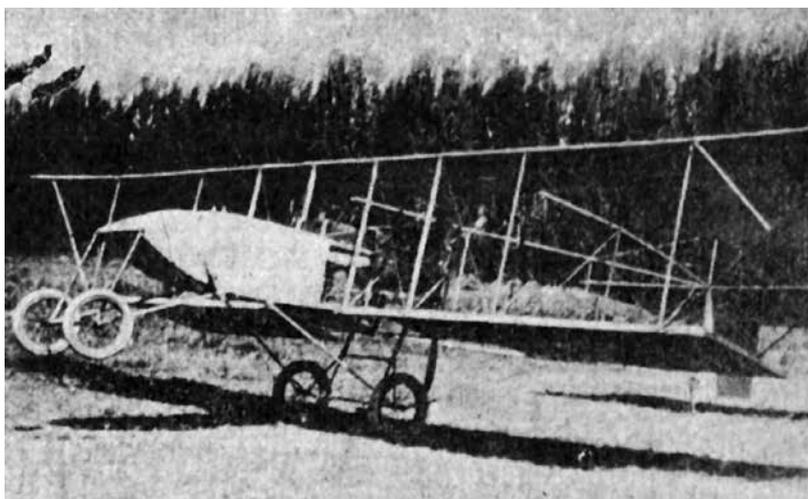
En el amplio período comprendido entre 1876 y 1894, el estadounidense Eduardo Laiselle, integrante de una compañía de acrobacias, logró hacer más de 150 elevaciones en Santiago y en otras ciudades locales. Después, este sujeto se enroló en el ejército que combatió contra peruanos y bolivianos en la Guerra del Pacífico (1879-1883) y luego también vio acción durante la Guerra Civil de 1891. Interesante sería saber si es que en algún momento Laiselle trasladó sus habilidades como aeronauta al campo de batalla en los desiertos del norte, y si es que durante las contiendas alguna vez un aerostato se elevó con alguna misión militar específica; hasta ahora no hay registro de aquello.

Aún con el éxito de la aerostación en Europa y de las certezas de su aplicación militar, los primeros observadores locales de las ventajas tácticas que se podrían derivar para el Ejército del empleo de estos ingenios ya daban señales de cierta visión muy objetiva. Así, la publicación *Revista Militar* (1.12.1887, p. 472) presentaba un artículo (Arredondo, N.) que sostenía que “*es indudable el hecho que los todos los inconvenientes que hasta la fecha puede haber presentado o presenta la navegación aérea por medio de globos tiene por causa el no poder ser dirigidos a voluntad por el que los gobierna; pudiéndose en consecuencia asegurar que no solo se subsanarían todos esos inconvenientes sino que los usos de ellos se multiplicarían si algún día se llega a conseguir su dirección*”.

Finalmente, para la celebración del primer centenario del inicio del proceso independentista nacional (1910) se produjeron en Santiago dos acontecimientos notables: la visita del aeronauta y trapecista colombiano Domingo Valencia, quien hizo varias ascensiones, y el vuelo en globo de la primera mujer chilena en hacerlo, la señorita Inés Clark.

## 1910: Debuta la aviación en Chile

Fue también con motivo de conmemorarse en septiembre de 1910 el primer centenario de la iniciación de nuestro proceso independentista, que la planificación de las actividades festivas en torno a este acontecimiento incluyó la posibilidad de la elevación de una aeronave en forma. Para tal efecto, los ciudadanos locales David Echeverría y Miguel Covarrubias decidieron hacer algunos vuelos demostrativos pagados, empresa para la cual adquirieron en Francia un avión Voisin de 50 hp. Para las pruebas de rigor, la empresa contrató a César Copetta, un francés residente, quien, el 21 de agosto de 1910, en los preparativos de las celebraciones oficiales, logró remontar el vuelo en el sector sur oriente de Santiago. Este evento se reconoce como la primera elevación en Chile de un aparato más pesado que el aire.



**Voisin militar chileno**

En las postrimerías del mismo año, procedente de Europa y para hacer algunas exhibiciones, visitó Santiago el aviador italiano Bartolomé Cattaneo. Equipado con un Blériot de 50 hp, este aviador hizo varias demostraciones en diciembre, a las cuales asistieron -entre varios otros miles de nacionales- un par de impresionados jóvenes oficiales de Ejército: Manuel Ávalos Prado y Eduardo Molina Lavín.

Cabe recordar que fue también en 1910 que falleció en un accidente en el Atlántico norte quien habría sido el primer aviador de sangre chilena, el señor Cecil Grace. Éste, nacido en la ciudad de Viña del Mar en 1886, a sus 6 años de edad había sido llevado a vivir a Inglaterra, y en su juventud se convirtió en el cuarto aviador graduado en tierras británicas. En diciembre de 1910 murió al intentar el cruce del Canal de la Mancha desde la isla al continente, mientras trataba de ganar un premio en dinero al aviador que lograra superar esa prueba.

## El interés militar: visionarios oficiales chilenos y nuestros primeros aviadores y mecánicos

En 1909 correspondió al general Arístides Pinto Concha, a la sazón Inspector de los Establecimientos de Instrucción del Ejército de Chile, ordenar al teniente coronel Mariano Navarrete, delegado militar en Francia, que hiciera los primeros informes respecto de las posibilidades reales de establecer la aviación militar en Chile. Navarrete propuso la creación de un servicio de aviación autónomo que estuviera compuesto por sendas secciones de globos, dirigibles y aviones.

En mayo de 1910 viajó a Francia el oficial ingeniero teniente coronel Pedro Pablo Dartnell, quien a su vez recibió de parte del general artillero Roberto Silva Renard, adicto militar en Alemania y jefe de los oficiales chilenos destacados en Europa, la orden de elaborar un informe definitivo que abordara la posibilidad de establecer la aviación militar en Chile. En diciembre del mismo año, y luego de haber visitado las principales casas constructoras locales y conversado con los sujetos más ilustrados y versados en aviación, Dartnell presentó su informe, macizo documento en el que se vertieron novedosos y visionarios conceptos en torno a la cuestión aeronáutica. Algunas de sus conclusiones fueron:

- Comprar solo aviones para el servicio militar, no globos; enumeró y describió los mejores aparatos disponibles para Chile;
- Favorable apreciación acerca del uso de los aeroplanos en las guerras del futuro y de su posibilidad de ser armados;
- La posibilidad real del uso de aviones de “observación, comunicación y combate” dentro del Ejército;
- Destacó la importancia crucial que debería darse a la formación de mecánicos y especialistas terrestres.

Adicionalmente, en similares fechas otros oficiales nacionales también elaboraron sendos informes positivos (comandante Julio Brownell, adicto en Francia, sobre la organización militar aérea francesa, y comandante Alfredo Schonmyer, adicto en Gran Bretaña, sobre el estado de la industria inglesa).

Fue también a fines de 1910 que el ya mencionado general Arístides Pinto Concha, actuando ahora como Ministro de Guerra y Marina, designó en Santiago a una comisión militar destinada a pronunciarse acerca de la posibilidad de adquirir aviones para el Ejército. En 1911, Pinto Concha fue designado presidente de la Comisión Militar Chilena en Europa, trasladándose en febrero hacia el Viejo Continente. Paralelamente, dos oficiales de Ejército eran comisionados a la Escuela Blériot en París para recibir instrucción de vuelo: los ya mencionados Ávalos y Molina. En julio del mismo año, estos dos militares recibieron sus brevet de pilotos por parte de la Federación Aeronáutica Internacional y -también ese año- Ávalos recibía para Chile el primer avión militar: un Blériot de 50 hp llamado “Manuel Rodríguez”. Sería en este aparato que ese año se realizaría en Francia el primer vuelo de un avión chileno luciendo las escarapelas nacionales.

De vuelta en Chile luego de su comisión europea, en 1912 el general Pinto Concha concluyó:

- Proponer un plan de desarrollo aeronáutico cuatrienal, a contar de 1913;
- Fundar una Escuela de Aeronáutica Militar y también toda la infraestructura necesaria para sostener el material aéreo;
- Formar en los años siguientes las respectivas compañías operativas de vuelo con los egresados de la Escuela;
- Crear una Inspectoría General de Aviación (dependiente del Ministerio de Guerra).

Luego de recibir otros aparatos, en noviembre de 1912 el capitán Ávalos regresó a Santiago para asumir interinamente la dirección de la Escuela de Aeronáutica Militar, establecimiento que se crearía en febrero de 1913.

Finalmente, los primeros mecánicos de Ejército que recibieron cursos en Europa en previsión de los servicios que deberían prestar para la Aviación Militar nacional fueron los señores Pedro Donoso y Miguel Cabezas, quienes lograron también convertirse en pilotos en 1913, año en el que regresaron a Chile a continuar prestando sus valiosos servicios.

## Nacimiento de la Aviación Militar y de la Escuela de Aeronáutica Militar



**Capitán Manuel Ávalos Prado**

Luego de todas estas actividades preliminares mencionadas, durante 1913 se fundan la Aviación Militar chilena y la Escuela de Aeronáutica Militar. El país entonces era gobernado por el Presidente de la República don Ramón Barros Luco (1910-1915).

Fue la Ley N° 2.771 de 1913 la que autorizó al Ejército para proceder a la creación de sus servicios aeronáuticos, siendo nombrado como Inspector General de Aeronáutica el general Aristides Pinto Concha, hecho que ocurrió en mayo del mismo año.

Por su parte, fue el Decreto Supremo N° 187 de 11 de febrero de 1913 el que dio nacimiento a la Escuela de Aeronáutica Militar.

Como Director de la Escuela el 22 de febrero del mismo año se designó originalmente al teniente coronel Carlos Hinojosa, quien se encontraba comisionado en Alemania y que, sin embargo, nunca ejerció el mando efectivo de dicha academia, siendo permanentemente reemplazado -hasta 1915- en calidad de interino por el propio capitán Ávalos.

En el área de mantenimiento y mecánica destacaron en esta etapa inicial los nombres de los pilotos mecánicos Miguel Cabezas, Pedro Donoso, Amadeo Schudek y Manuel Penelas. Como jefe de todos ellos actuaba el ingeniero naval don Pedro Andrade Moss.

La finalidad principal de la Escuela sería adiestrar oficiales y suboficiales como pilotos aviadores, pilotos mecánicos o pilotos aerostáticos para su servicio en el Ejército; para lograrlo, abrió la postulación para ingresar a ella a capitanes, tenientes 1° y 2° y suboficiales interesados, de cualquier arma que provinieran.

La Escuela se estableció en el terreno agrícola fiscal de Lo Espejo, usado hasta esa fecha para algunos menesteres propios de la policía de la época. Este sitio tenía unos 600 mil metros cuadrados de superficie, aunque carecía de las mejores características como centro de instrucción de aviación, debido a algunas estrecheces y al hecho de estar rodeado de árboles. Con el tiempo, la base fue creciendo hasta abarcar los terrenos aledaños del Regimiento de Ferrocarrileros y algunas extensiones del sector norte adquiridas a contar de 1918 en la chacra De Mabelle, año en que la aviación militar recibió una numerosa partida de aviones de guerra procedentes de Gran Bretaña y cuya operación segura requería un campo de mayores dimensiones.

## El primer curso de alumnos

Dadas las circunstancias mencionadas, el alto mando del Ejército hizo un llamado para quienes estuvieran interesados en ingresar a la Escuela y cumplieran con los requisitos básicos físicos, intelectuales y médicos exigidos. Se presentaron unos 60 candidatos, los que fueron examinados en una serie de materias por una comisión presidida por el propio general Pinto Concha, cuerpo colegiado que el 17 de marzo de 1913 dio su veredicto final, aceptando el ingreso de los siguientes oficiales y suboficiales:

### *Oficiales:*

Amadeo Casarino, Víctor Contreras, Alejandro Bello, Tucapel Ponce, Francisco Mery, Enrique Pérez, Armando Urzúa, Julio Torres, Gabriel Valenzuela y Arturo Urrutia.

### *Suboficiales:*

Adolfo Menadier, Juan Verscheure, Eleodoro Rojas, José García, Floridor González, Luis Omar Page y Manuel Ampuero

A comienzos de abril siguiente, cuatro oficiales y dos suboficiales de los mencionados fueron enviados por el gobierno a las escuelas Breguet y Sánchez Besa en Francia para obtener sus brevet de pilotos aviadores.

Los que se quedaron en Chile deberían aprender a volar enseñados por el propio capitán Ávalos, a la sazón el único piloto aviador militar existente en Chile. Los cursos que Ávalos impartió para los alumnos del primer curso que no fueron a Francia comenzaron también en abril de 1913.

## El material aéreo de la Escuela y los primeros vuelos



**Blériot XI y el perro Pegoud, mascota de los pilotos de la Escuela Aeronáutica Militar**

Mientras Ávalos estudió y aprendió sobre aviación en Europa (1911-1912) también examinó, adquirió y recibió los primeros cuatro aviones con que el gobierno dotó a la naciente Aviación Militar/Escuela. Estos aparatos fueron:

Blériot Escuela monoplaça de 35 hp llamado "Chile"

Blériot 50 hp llamado "Manuel Rodríguez"

Voisin de 70/75 hp llamado "José Robles"

Deperdussin de 70 hp llamado "Emisario Estay"

Con el avión "Chile" el 7 de marzo Ávalos efectuó el primer vuelo militar no oficial en el país, de prueba, sobre los terrenos de la Escuela. Por su parte, el primer vuelo militar oficial ocurrió días después, el 12 de marzo, con el avión "Manuel Rodríguez" y -como correspondía- ante altas autoridades nacionales. El piloto mecánico Miguel Cabezas también puso lo suyo este notable día, volando el Voisin de 70/75 hp.

Durante el transcurso de 1913 la Escuela comenzó a recibir material aéreo adicional procedente de Francia, en la forma de:

1. Dos Blériot XI tandem de 80 hp;
2. Dos Blériot XI monoplaças de 50 hp;
3. Tres Blériot Escuela 35 hp;
4. Dos Blériot "Pingüinos" de 25 hp;
5. Tres Breguet Type III biplanos de 80 hp;
6. Un Breguet Type G.2 bis biplano de 100 hp (con alguna aplicación como bombardero);
7. Dos Sánchez Besa de 80 hp (y en proceso de entrega otros tres de guerra y uno Escuela).

Este fue, entonces, el primer material aéreo de la aviación militar chilena.

Durante la secuela de 1913 imperó en Chile la *escuela francesa* de enseñanza aeronáutica (caracterizada por el empleo de aviones con escasa aplicación militar y sin doble comando para alumno e instructor, entre otras características).

Los alumnos debían instruirse unos tres meses antes de realizar su primer vuelo solo. El grupo de alumnos que quedó en Chile empezó sus pruebas de graduación como pilotos aviadores en agosto de 1913, en una serie de pruebas públicas llevadas a cabo en Lo Espejo. Hacia diciembre siguiente, todos los ingresados a la Escuela estaban graduados como pilotos aviadores y seguirían acumulando horas de vuelo y experiencia para optar esta vez al título de pilotos militares.

Como características notables del período, toda la Escuela se presentó en vuelo el 19 de septiembre de 1913 sobre Santiago, en el día de las Glorias del Ejército, y también se ejecutaron una serie de vuelos destinados a aventurarse hacia otras ciudades cercanas a la capital, más allá de los simples extramuros del instituto formador.

A fines de 1913 el país ya contaba con los primeros pilotos aviadores militares y la Escuela podía mostrar a la comunidad y al alto mando un palmarés de casi 30.000 kilómetros volados y cinco pilotos militares y tres pilotos aviadores graduados, entre otros méritos. Recordemos los nombres de nuestros primeros cinco pilotos aviadores militares: capitán Ávalos, teniente Urzúa, teniente Mery, teniente Pérez y sargento Page.

El esquema general de trabajo de la Escuela se mantendría casi sin variaciones hasta la nueva época iniciada durante 1918, con la finalización de la influencia de la *escuela francesa* y la llegada de la primera misión inglesa a la aeronáutica militar chilena -encabezada por el capitán de la RAF Victor Huston-, delegación que tuvo amplias y naturales repercusiones para el desarrollo de las alas militares. La Aviación Militar subsistiría como tal hasta el 21 de marzo de 1930, fecha en la cual fue fusionada con el Servicio de Aviación Naval (originado en 1919), dando lugar a la Fuerza Aérea Nacional, posteriormente conocida como Fuerza Aérea de Chile.

En lo que se refiere estrictamente a la aviación militar del Ejército, el mando de esta institución dispuso en 1965 que personal dependiente de la Dirección de Operaciones del Estado

Mayor General, la Academia de Guerra y del Club Aéreo del Personal del Ejército (fundado en 1959) se abocara a diseñar, fundamentar y proponer las bases para la definitiva reactivación de la especialidad de aviación. Esos estudios y trabajos culminaron con la dictación del Decreto Supremo N° 267, de 16 de noviembre de 1970, el que creó, a partir del 1° de octubre de ese mismo año, el nuevo Comando de Aviación del Ejército (CAVE), reanudándose así formalmente la actividad aérea del Ejército de Chile después de un largo paréntesis de 40 años. □

## Bibliografía

- BRAHM, Enrique (2003). *Preparados para la guerra. Pensamiento militar chileno bajo influencia alemana 1885-1930*. Ediciones Universidad Católica de Chile (Santiago).
- CONTRERAS, Víctor (1916). *Historia de la aeronáutica militar de Chile*. Imprenta Universitaria (Santiago).
- FLORES, Enrique (1933). *Historia de la aviación en Chile*. Tomo I. (Santiago).
- FLORES, Enrique (1950). *Historia aeronáutica de Chile*. (Santiago).
- COMANDANCIA EN JEFE, FACH (1999). *Historia de la Fuerza Aérea de Chile*. Tomo I (Santiago).



**El Señor Iván Siminic** es un Investigador del Departamento de Investigación y Extensión de la Academia de Guerra Aérea de la Fuerza Aérea de Chile. Autor de numerosos artículos relativos al estado y empleo del poder aéreo y sobre temas del ámbito de las relaciones internacionales. Autor de los libros “36 AÑOS DE AVIONES JET EN LAS AEROLÍNEAS CHILENAS, 1964-2000” y “EL AVIÓN LAN 18 Y LOS FAIRCHILD FC-2 EN CHILE”, publicados en 2000 y 2009. Autor de los libros “*El avión Capitán Pastene, crónica de un regalo que se frustró*” (2002), y “*DE LA NARANJA MECÁNICA Y OTRAS HISTORIAS: LA AVIACIÓN EN LA POLICÍA CIVIL CHILENA DESDE 1962*” (inédito). En 2011 la misma Academia le publicó el libro de su autoría “*CAMPAÑAS AÉREAS EN LAS GUERRAS DE COREA Y VIETNAM*”, y en 2012 hizo lo propio con el libro “*MALVINAS 1982. HISTORIA DEL CONFLICTO. LA GUERRA AÉREA*”. En marzo de 2012 la FACH lo distinguió con la condecoración DIEGO ARACENA AGUILAR, por sus trabajos de investigación y por su contribución académica.

# Observaciones sobre la Guerra Aérea en Siria

TENIENTE CORONEL S. EDWARD BOXX, USAF

*Su rostro estaba ennegrecido, sus ropas deshilachadas. No podía hablar. Solo apuntaba hacia las llamas, a unas cuatro millas, entonces susurró: “Aviones . . . bombas”.*

—Sobreviviente de Guernica

**G**IULIO DOUHET, Hugh Trenchard, Billy Mitchell y Henry “Hap” Arnold fueron unos de los más grandes teóricos de poderío aéreo en la historia. Sus reflexiones han inequívocamente formado la base del poderío aéreo moderno.<sup>1</sup> Sin embargo, sus ideas con respecto al uso más eficaz del poderío aéreo no fueron en modo alguno ni uniformes ni congruentes en su determinación de qué consistía un centro vital con efectos estratégicos. De hecho, el debate continúa hasta la fecha, y uno podría referirse a conflictos recientes en el Oriente Medio para hacer observaciones sobre el tema. Específicamente, en este artículo se analizan las acciones de unas de las fuerzas aéreas más grandes del mundo en su lucha contra su propio pueblo—a saber, los rebeldes del Ejército Libre de Siria (FSA, por sus siglas en inglés).

A principios del 2013, la guerra civil siria actual ha resultado en más de 60.000 muertos, 2,5 millones de personas expatriadas y más de 600.000 refugiados en Turquía, Jordania, Irak y el Líbano.<sup>2</sup> El Presidente Bashar al-Assad ha mantenido su postura en parte a causa de su capacidad de controlar los cielos y atacar blancos de la oposición—inclusive civiles.<sup>3</sup> Las tácticas de la Al Quwwat al-Jawwiyah al Arabiya as-Souriya (Fuerza Aérea Siria) parecen recordar las de la Guerra Civil Española, cuando los bombarderos de la Legión Cóndor alemana atacó el pueblo vasco basado en el comercio de Guernica, España, el 26 de abril de 1937. Este bombardeo intencional de una población civil escandalizó al mundo; más tarde, Pablo Picasso captó el incidente en su famoso mural *Guernica*.

Hoy el caso sirio evoca recuerdos del teórico italiano de poderío aéreo, Giulio Douhet, quien opinaba que los bombardeos aéreos podían destruir el estado de ánimo de los civiles, aclarar la base social de la resistencia y aterrorizar grandes porciones de poblaciones civiles.<sup>4</sup> Aunque la mayoría de los militares occidentales modernos se esfuerzan al máximo para perfeccionar las municiones de precisión y las tácticas concebidas para limitar las bajas de civiles, análisis iniciales revelan un método muy diferente en Siria. De hecho, las acciones del régimen al-Assad probablemente se registrarán como un recuerdo deprimente de los abusos que regímenes totalitarios hizo posible e implantaron, recordando los principios pronosticados hace más de un siglo por Douhet y otros. Si bien es una narrativa macabra, el uso del poderío aéreo en Siria exige un análisis, inclusive mientras la lucha continúa. Por lo tanto, en este artículo se ofrecen algunos comentarios sobre las dos últimas décadas de guerra civil.

Evidentemente, el régimen sirio adoptó las premisas mayores de Douhet y utilizó el poderío aéreo para atacar civiles primero por medio de helicópteros y luego con aeronaves de ala fija, inicialmente permitiéndole a las fuerzas de al-Assad que impidieran los avances del FSA y demorar el derrumbe del régimen. Sin embargo, los rebeldes se han adaptado a la amenaza, empleando mejores tácticas y armamento antiaéreo más eficaz, y desde entonces han disfrutado un mayor grado de éxito táctico. Este análisis comienza con una breve historia del surgimiento del régimen al-Assad y luego trata la creación e intensificación de la fuerza aérea siria al igual que los acontecimientos que condujeron al conflicto actual. En él se destacan observaciones que apun-

tan a la conclusión que el régimen adoptó la teoría douhetiana básica ya que llevó a cabo una campaña aérea contra las fuerzas rebeldes.

## Antecedentes

Los sirios celebraron el Día de la Independencia el 17 de abril de 1946, “fecha en el que último soldado francés abandonó el suelo sirio”.<sup>5</sup> La fuerza aérea siria se formó en el 1948, poco después que Estados Unidos crease su propia fuerza aérea. El servicio embrionario de la era de los años cincuenta poderosamente le dio forma al futuro presidente Hafiz al-Assad—padre del actual presidente—quien consolidó el poder en Siria el 16 de noviembre de 1970 y gobernó hasta su muerte en el 2000. Su personalidad y dictadura estaban atadas muy de cerca con la fuerza aérea siria y, a su vez, la convirtió en una de las armas aéreas más grandes en el Oriente Medio.

En calidad de ex piloto de combate, comandante de escuadrón, comandante de fuerza aérea y ministro de defensa, al-Assad adoptó el poderío aéreo junto con tanques, artillería y capacidades de misil. En 1951 fue uno de 15 cadetes seleccionados para el entrenamiento de vuelo en Aleppo. Se convirtió en un piloto consumado, sobreviviendo múltiples accidentes casi fatales e inclusive intentando trabar combate con un avión de reconocimiento Canberra británico durante la crisis de Suez de 1956.<sup>6</sup> Al-Assad fue uno de los pocos oficiales sirios seleccionados para asistir al entrenamiento en los aviones de combate MiG-15 y MiG-17 en la Unión Soviética en 1958 y más tarde estuvo al mando de un despliegue de aviones de combate a Egipto.<sup>7</sup> La fuerza aérea siria le ofreció una oportunidad para un avance social e intelectual—especialmente importante ya que él era oriundo de la minoría alawita, a menudo perseguida, que comprendía el 14 por ciento de la población siria y considerada por algunos musulmanes como la ramificación hereje del Islam.<sup>8</sup>

En calidad de presidente, al-Assad colocó miembros de su secta religiosa en puestos importantes en la fuerza aérea, una técnica que más tarde su hijo copió. En el conflicto actual, Bashar al-Assad hábilmente ha convencido a sus conciudadanos alawitas que su futuro está atado a su supervivencia. Tal como se comprueba durante la guerra civil actual, un escenario que incluye una minoría que percibe una lucha existencialista mientras que está al mando de una fuerza aérea grande y moderna puede tener consecuencias desastrosas para los civiles.

## Las semillas de la disidencia

*Nos tropezamos con un anciano de hombros encorvados...que estaba que arrastraba sus pies en este campo de muerte.*

*“¿Dónde están todas las casas que estaban aquí?” nos detuvimos y le preguntamos.*

*“Están conduciendo sobre ellas,” respondió.*

*“Pero, ¿dónde están las personas que vivían aquí?” dije.*

*“Quizás también esté manejando sobre algunas de ellas”, balbuceó y continuó alejándose arrastrando sus pies.*

—Thomas Friedman, corresponsal del *New York Times*  
Hama, Siria, 1982

En 1982, una revolución suní encabezada por la Hermandad Musulmana Siria retó significativamente al gobierno de Hafiz al-Assad. La reacción militar subsiguiente de mano dura presagió su uso devastador del poderío aéreo en la actualidad. La rebelión consistía de las tres ciudades más grandes de Siria: Aleppo, Homs y Hama, comunidades de mayoría suní que más adelante

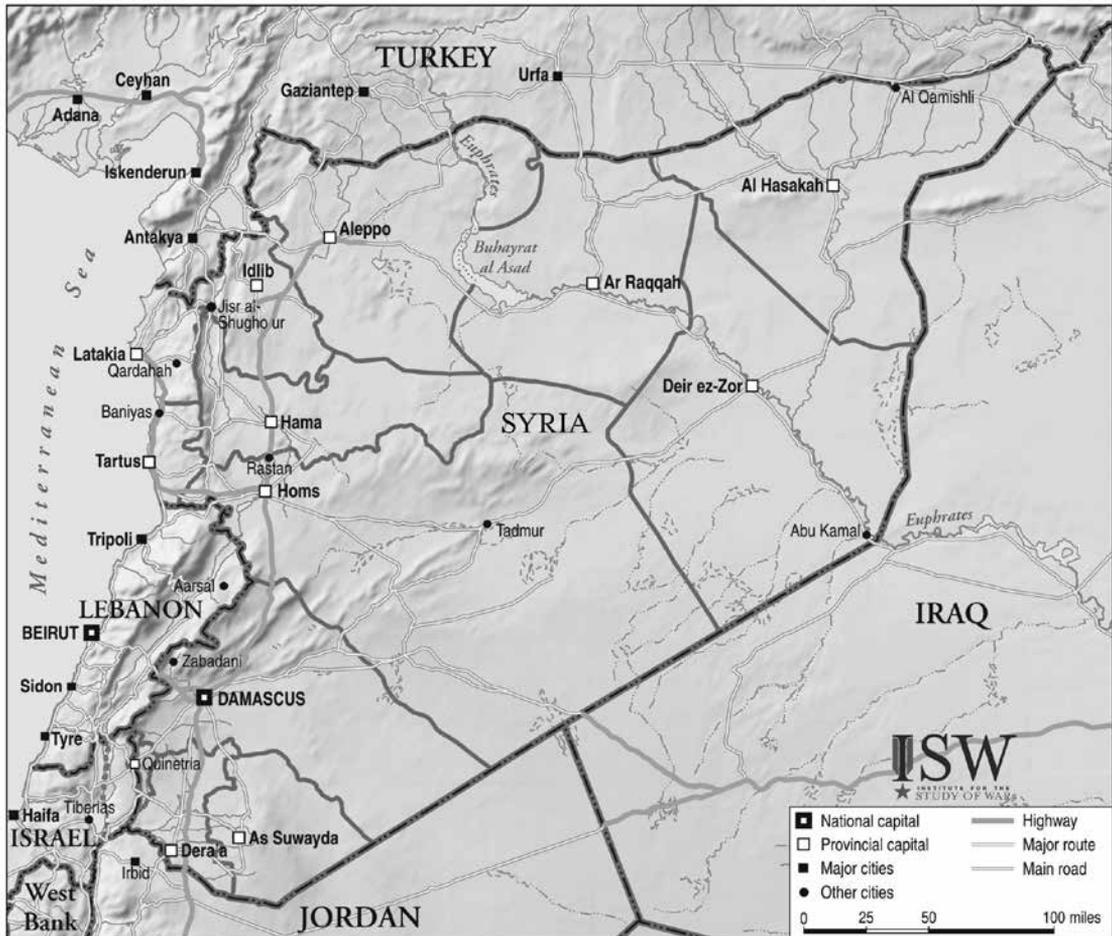
serían testigos del conflicto al oponerse a al-Assad durante la guerra civil. En su libro, *From Beirut to Jerusalem* (De Beirut a Jerusalén), su obra transcendental sobre el levante (*Levant*), Thomas Friedman evaluó las medidas severas de al-Assad en cuanto al levantamiento suní que pudo haber matado casi tantos sirios, principalmente en Hama, como la actual guerra civil.<sup>9</sup> En aquel entonces como ahora, uno encuentra las tácticas de destruir vecindarios completos e hitos históricos, no tan solo para aplacar el levantamiento sino también para recrear venganza generacional. Como resultado de políticas tribales, las acciones de los alawitas reflejaron una creencia de que la crueldad estaba ligada con su supervivencia contra los sunís más numerosos, justificando sus técnicas contrarrevolucionarias devastadoramente draconianas. De hecho, el uso autoritario de la milicia de Hafiz al-Assad contra los civiles destaca las consecuencias de contar con un grupo selecto que gobierne la milicia o una fuerza aérea.<sup>10</sup>

Además al-Assad interpretó el deseo de algunos sirios de contar con estabilidad, indistintamente del costo, como aprobación tácita de sus métodos. Si bien es una de las áreas pobladas más antiguas del mundo, Siria es un país joven políticamente hablando, y el régimen se aprovechó del nacionalismo del partido Baath para acusar a los rebeldes sunís de dividir el país. Al igual que su padre, Bashar al-Assad ahora intenta representar toda la oposición armada como foráneos, terroristas y una amenaza existencial para Siria.<sup>11</sup> Inclusive algunos que no son alawitas preferirían un gobierno estable a una teocracia islámica o un sistema marcado por un conflicto sectario interminable, como el que a menudo experimentó el país vecino del Líbano.<sup>12</sup> Los numerosos paralelos con la masacre de Hama décadas anteriores puede que ayuden a explicar las tácticas hobbesianas empleadas por la fuerza aérea siria en la actualidad.<sup>13</sup>

## La guerra civil

El levantamiento popular actual, conocido como “el Día de la Furia” comenzó el 15 de marzo de 2011, cuando los disidentes se arrojaron a las calles alrededor del país, respondiendo en parte al encarcelamiento a inicios de la semana de jóvenes menores de 15 años quienes escribieron que “el pueblo quiere derrocar al régimen” en una pared en Deraa.<sup>14</sup> Para el mes de abril, el régimen había adoptado y método agresivo, utilizando tanques, compañías de infantería y artillería pero no aeronaves. Las protestas se esparcieron por Siria, pero las dos ciudades más grandes—Damasco y Aleppo (fig. 1)—no fueron afectadas al principio. (Damasco, la sede del poder, y Aleppo, el centro de la población, son dos de los lugares continuamente habitados por más tiempo en el mundo.)<sup>15</sup> Pero poco después las fuerzas de al-Assad sellaron y atacaron ciudades tales como Deraa, en el sur, y Latakia, al oeste.<sup>16</sup> A inicios de junio de 2011, Jisr al-Shughour, una ciudad al noroeste—una encrucijada estratégica entre Aleppo y la costa del Mediterráneo en el histórico Río Orontes—fue testigo de una emboscada de 20 tropas sirias, ya sea por rebeldes y habitantes o por tropas sirias que desertaron.<sup>17</sup>

Según el Dr. Radwan Ziadeh, portavoz para la oposición siria, julio de 2011 marcó el establecimiento de la resistencia militar oficial al régimen de al-Assad.<sup>18</sup> A medida que la competencia de la oposición armada de Siria aumentó, la milicia siria tuvo que emplear armamento más pesado contra los rebeldes. Para enero de 2012, el régimen había iniciado operaciones de artillería a gran escala a lo largo de Siria. En abril de ese año, al-Assad reaccionó a victorias inesperadas del FSA en Idlib y Aleppo enviando helicópteros para atacar las aldeas “liberadas”.<sup>19</sup> Hacia fines de mayo de 2012, a medida que la oposición montó ofensivas, el régimen comenzó el uso consistente de helicópteros armados para compensar por su movilidad reducida a causa de la interdicción eficaz con bombas y emboscadas de los caminos por parte de los rebeldes. Este incremento en el empleo de helicópteros culminó el 12 de julio durante una masacre en la aldea de Trenshe. Guiados por los preceptos principales de la teoría de Douhet, los helicópteros bombardearon y los *Shabiha* (árabe para “fantasmas”) (milicias irregulares) atacaron la ciudad de 7.000 habitantes.



**Figura 1. Ciudades y líneas de comunicación principales en la Siria de la guerra civil.** (Reproducida con permiso del Instituto para el Estudio de la Guerra, consultado el 1º de febrero de 2013, <http://www.understandingwar.org/sites/default/files/ISWSyriaBaseMap%20copy.png>.)

En agosto de 2012, el régimen comenzó a emplear aviones a reacción en un rol de interdicción a medida que las líneas de batalla en Aleppo se intensificaron y el uso de helicópteros por parte del régimen alcanzó su máximo. Puede que al-Assad haya ordenado el uso de plataformas de ala fija por los problemas de mantenimiento relacionados con operar aproximadamente 50 helicópteros y la falta de helicópteros de ataque *Mi-25 Hind* sumamente capaces. El *Mi-25* (la versión exportada del *Mi-24* ruso) aparentemente estaba reservado para zonas importantes de la oposición—principalmente, Jabal al-Zawiya, un trecho de autopista impugnado en Idlib, y las zonas de Rastan y Talbiseh de Homs. El empleo de aviones de combate en los bombardeos y ametrallamientos por parte de la fuerza aérea siria rápidamente superó el uso diario de helicópteros en términos de incursiones.

La capacidad de defensa aérea cada vez mayor de los rebeldes, que obligaron al régimen a operar a altitudes más elevadas, también representa la transición de aeronaves de ala giratoria a ala fija. La oposición respondió al poderío aéreo del régimen derribando una cifra limitada de

aeronaves y atacando bases aéreas. Para fines del verano de 2012, el equipo de los rebeldes probablemente incluía de 15 a 25 ZU-23, dos a cinco ametralladoras remolcadas de artillería antiaérea (u otras) de 57 mm y 15 a 30 SA-7 sistemas portátiles de defensa aérea (MANPADS, por sus siglas en inglés).<sup>20</sup> Informes también indican la presencia de misiles de superficie a aire (SAM, por sus siglas en inglés) SA-16 y SA-24. Los rebeldes dependían principalmente de ametralladoras antiaéreas pesadas como la ZU-23 y, al menos en una ocasión, un MANPADS.<sup>21</sup> A partir de octubre de 2012, el FSA había derribado aproximadamente cinco aeronaves de ala giratoria y seis de ala fija, al menos siete vídeos confirman el éxito de los rebeldes. Metrajés no corroborados muestran el derribo de aeronaves y helicópteros e inclusive pilotos de combate capturados y escombros de aeronaves. En otros informes, la cifra de aeronaves derribadas es más elevada, 19; sin embargo, los vídeos del FSA y las afirmaciones son difíciles de verificar.<sup>22</sup>

Además, el FSA inicialmente trató de invadir bases aéreas del régimen, inclusive aquellas en Abu ad Duhur (al sur de Aleppo), Minakh (al norte de Aleppo y sede de más de cuarenta helicópteros Mi-8), Taftanaz (otra base de helicópteros cerca de Aleppo) y al-Qusayr (cerca de Homs). Presuntamente, los rebeldes atacaron esas bases aéreas para aprovecharse de la vulnerabilidad de las aeronaves en tierra y durante el despegue y aterrizaje. Cuatro de los ataques exitosos a las aeronaves ocurrieron cerca de esas bases militares.<sup>23</sup>

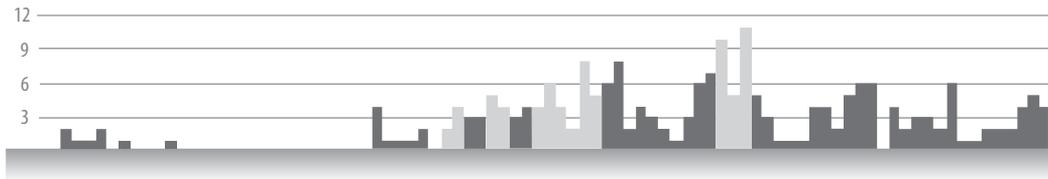
Durante el conflicto, el régimen sirio dependió de armamento pesado (artillería de campaña, morteros y cohetes) como el medio principal para reprimir la rebelión. Luego empleó cada vez más el poderío aéreo para desacelerar el avance del FSA, según se mostró a fines de octubre durante el cese de fuego propuesto por el día feriado musulmán, Eid al-Adha. En lugar de disminuirlos, los ataques aéreos del régimen en realidad aumentaron significativamente, de un promedio de 20 a 25 ataques aéreos por día a más de 60, tan solo el 29 de octubre. Durante ese mes, la lucha entre el FSA y las fuerzas de al-Assad alcanzaron un punto culminando con un cálculo de 764 enfrentamientos reportados—la cifra más alta desde que la guerra comenzó.<sup>24</sup> Indistintamente del motivo por el cambio, el uso acelerado del poderío aéreo fue indicio de una ofensiva terrestre en decadencia por parte de las fuerzas del régimen.

## ¿Atacar civiles?

Para septiembre de 2012, muchos observadores internacionales opinaban que la fuerza aérea siria estaba atacando civiles, principalmente empleando sus aeronaves en una manera punitiva y vengativa en lugar de una táctica.<sup>25</sup> Pruebas empíricas y observaciones en una de las guerras civiles más grabadas en vídeo en el mundo indican que la mayoría de los ataques aéreos del régimen han sido en ciudades y vecindarios donde los rebeldes se han apoderado del control, en lugar de sitios militares rebeldes específicos.<sup>26</sup> Los más de trece bombardeos que ocurrieron mientras que civiles esperaban en fila en reposterías y prensas de aceitunas comunitarias durante la cosecha ilustran su vulnerabilidad a los ataques aéreos.<sup>27</sup> Para octubre de 2012, ya era obvio que la fuerza aérea siria no pretendía evitar las bajas de civiles cuando atacó ciudades que contenían fuerzas rebeldes (fig. 2).<sup>28</sup>

Además, el régimen ha empleado sus 17 helicópteros *Mi-8* para lanzar tanques viejos de almacenamiento o cilindros de metal cargados con explosivos y chatarra metálica—“bombas de barril”—desde los helicópteros. Nadie sabe si la fuerza aérea empleó esta táctica para maximizar la funcionalidad múltiple de sus helicópteros o para ahorrar municiones de fábrica para los aviones de reacción de ataque. Indistintamente, el empleo a gran altitud de estas “bombas” evidentemente aterrorizaba a la población civil con buenos resultados. Un refugiado sirio describió las bombas como tan grandes que “aspiraban el aire y todo se desplomaba, inclusive edificios de cuatro pisos”.<sup>29</sup>

## Ataques con aeronaves de ala giratoria:



## Ataques con aeronaves de ala fija:



Amarillo indica días que incluyen ataques aéreos contra puestos rebeldes.

Rojo indica días que incluyen ataques aéreos contra puestos no rebeldes.

Cronología ilustra del 1º de abril al 1º de octubre de 2012

**Figura 2. Ataques aéreos contra el FSA, 1 de abril a 1 de octubre de 2012** (Reproducido con permiso de Joseph Holliday y Christopher Harmer, *Syrian Air Force and Defense Overview* (La fuerza aérea siria y resumen de la defensa) [Washington, DC: Institute for the Study of War (Instituto para el estudio de la guerra), 25 de octubre de 2012], 4, <http://www.understandingwar.org/press-media/graphsandstat/syrian-air-force-air-defense-overview>.)

## La fuerza aérea Siria

Para fines del verano de 2012, el régimen probablemente contaba con no más de 200 aeronaves con capacidad de combate—aproximadamente 150 aviones de reacción y 50 helicópteros—de los 600 en su inventario total antes de la guerra civil, e inclusive esos tenían varios grados de capacidad de combate. Además, en virtud de las deficiencias en el mantenimiento histórico, combinadas con el ritmo de las operaciones, el régimen al-Assad probablemente no puede emplear más del 30 al 50 por ciento de sus aeronaves.<sup>30</sup> Puede que la fuerza aérea haya reservado sus *MiG-25*, *29* y *Su-24* de mejor calidad en preparación para una intervención externa—pero también puede que no haya podido utilizar estos diseños de aire a aire en funciones de aire a tierra. Por ejemplo, el *MiG-25*—conocido como una “tabla de planchar voladora” por sus interceptaciones a gran altitud en lugar de maniobras a bajo nivel—verdaderamente no está diseñado para una función de aire a tierra. Los líderes sirios puede que también estén preocupados acerca de más desertiones. Un piloto sirio de *MiG-21* hizo una desertión muy publicada hacia Jordania en junio de 2012; además, informes desde adentro de la fuerza aérea revelan que los pilotos no alawitas deben permanecer en las barracas y que solamente los pilotos alawitas “autorizados” pueden volar, lo que indica que más pilotos de combate desertarían si se les diese la oportunidad.<sup>31</sup>

Al igual que muchas fuerzas aéreas modernas, la de Siria no estaba preparada para combatir una insurgencia, habiéndose enfocado principalmente en una posible amenaza israelita, lo que explica la nueva función del avión *L-39* (*Albatross*) no como entrenadores (su función principal) sino como plataformas de apoyo aéreo cercano. El uso sorpresivo de los *L-39* puede que haya resultado del hecho de que tiene menos problemas de mantenimiento que los melindrosos aviones de reacción *MiG*, su rendimiento comparativamente mejor a altitudes y velocidades aerodi-

námicas más bajas o sencillamente la presencia de más pilotos expertos y cómodos con un avión entrenador

En enero de 2012, la fuerza aérea siria intentó comprar de Rusia 40 entrenadores *Yak-130*, pero en julio de 2012, bajo presión de Washington y de las Naciones Unidas, Rusia no entregó los aviones prometidos.<sup>32</sup> Este interés en estas aeronaves avanzadas entrenadoras de combate correspondió con el aumento en el uso de los entrenadores L-39, probablemente reflejando el deseo del régimen de emplear más aeronaves de ataque terrestre. Para fines de noviembre de 2012, los Su-17 y Su-22 *Fitters* aparecieron por primera vez en la guerra. Los expertos opinan que un incremento en la iniciativa de mantenimiento y un inventario grande le permitió al régimen lograr que unos cuantos de esos aviones se pudiesen volar y por ende introducirlos en el conflicto.<sup>33</sup>

## Defensas aéreas Sirias

Al inicio de la guerra civil, la red de defensa aérea de Siria se consideraba entre las más capaces y densas en el mundo, quizás superada solamente por las de Corea del Norte y Rusia. Estas defensas de capas múltiples y la amenaza de armamento químico lanzados desde *Scuds* eran dos inquietudes importantes durante el debate interinstitucional sobre una zona de no vuelo encabezada por Estados Unidos. Ubicada principalmente a lo largo del corredor Damasco-Homs-Aleppo (ver fig. 1) y la costa del Mediterráneo, la cobertura superpuesta de los misiles y radares consistía de aproximadamente 650 emplazamientos estáticos de defensa aérea, el más preocupante de los cuales era el que alojaba el SA-5 “*Gammon*”, que tenía un alcance de 165 millas náuticas y una capacidad de altitud de 100.000 pies. Las plataformas sirias también incluían más de 300 sistemas de defensa aérea portátiles, los más capaces de los cuales incluían los SA-11 y SA-17 más nuevos, al igual que los misiles anti-cruceros y anti-furtivos, SA-22. El derribo de un avión de combate F-4E turco cerca de Latakia el 33 de junio—aunque la causa del accidente aún se desconoce—realizó la letalidad percibida del sistema de defensa aérea de al-Assad.

Por otra parte, los sistemas de defensa aérea legados de fabricación rusa de Siria tenían limitaciones. Un avión de reacción ruso rumbo a Siria desviado por Turquía supuestamente transportaba repuestos sumamente necesarios. Además, la Organización del Tratado del Atlántico Norte y la fuerza aérea israelí han penetrado y contenido repetida y eficazmente los sistemas rusos. De hecho, el conflicto interno ha degradado significativamente la eficacia de las defensas aéreas sirias. Al igual que las fuerzas terrestres, el ausentismo y las deserciones han acosado el apresto de los sistemas de misiles y radares sirios. Durante el año pasado, el FSA ha capturado lanzadores SA-2 y SA-8 y ha invadido sitios e instalaciones de SA-2, SA-3 y SA-5.<sup>34</sup> Hacia fines de octubre de 2012, a medida que los rebeldes consolidaban las conquistas en el norte en la provincial Idlib, las fuerzas sirias tuvieron que destruir algunos de sus SAM para evitar que cayeran en manos del FSA.<sup>35</sup> Para diciembre de 2012, batallones del FSA acantonados en la gobernación de Damasco habían “logrado el control de la mayoría de las bases de defensa aérea en esa gobernación”.<sup>36</sup>

## Ventaja de los rebeldes

*Controlamos el 70% del cielo, porque si usted compara la situación ahora con la de hace dos meses, hay muchos menos aviones.*

—Khelif Abu Allah, un artillero Dushka  
Noviembre de 2012

A fines de noviembre e inicios de diciembre de 2012, la oposición siria adquirió ímpetu. La guerra estaba cerca de un impasse cuando de repente las fuerzas rebeldes atacaron múltiples bases aéreas, inclusive Marj al-Sultan en las afueras de Damasco, varias instalaciones terrestres importantes y la represa hidroeléctrica Tishreen cerca de la frontera con Turquía. Las victorias de los rebeldes en la lejana provincia de Dier al-Zour provocó que el gobierno se retirara de sus últimas bases en la ciudad Deir al-Zour (la sexta ciudad más grande de Siria), dejando a los rebeldes en control de los campos de petróleo sirios. Las fuerzas rebeldes ejercieron cada vez más presión sobre Damasco, inclusive el aeropuerto internacional del país.

Esos enfrentamientos exitosos ilustran la estrategia nueva y eficaz de los rebeldes. Primero, como una manera de impedir el poderío aéreo, se enfocaron en capturar las bases responsables por el lanzamiento de los bombardeos y los ataques aéreos. Los rebeldes cambiaron de intentar capturar y apoderarse de territorio dentro de las aldeas y ciudades porque las aeronaves sirias sencillamente regresarían y bombardearían el nuevo territorio adquirido y la población civil. A diferencia de lo que ocurrió anteriormente, los rebeldes se dispersaron rápidamente para evitar convertirse en blancos concentrados para las aeronaves que contraatacaban. El cambio en las tácticas también constituyó un intento de recobrar el apoyo en decadencia del pueblo: los rebeldes y civiles por igual se percataron que el territorio capturado—especialmente zonas urbanas con poco o ningún valor militar—invitaban un asalto aéreo devastador por parte del régimen.<sup>37</sup> Retener esas áreas resultó demasiado costoso, enemistando a los civiles quienes soportaban la peor parte de los contra asaltos aéreos—exactamente la intención del régimen sirio (o sea, mostrarle a la población que apoyar a los rebeldes dejaba a los civiles expuestos).

Segundo, los rebeldes utilizaban sus bases aéreas como depósitos vitales de abastecimiento para obtener armamento pesado y armamento antiaéreo, creando así una defensa *ad hoc*, de baja altitud y en capas mediante ametralladoras y MANPADS. El FSA adquirió más sistemas de misiles lanzados desde el hombro, tanto como 40 de ellos, durante las ofensivas reanudadas en el otoño y derribó dos helicópteros y un avión de reacción en la provincia de Aleppo la primera semana de diciembre.<sup>38</sup> Un vídeo de uno de los ataques publicados en línea muestra lo que parece ser un SAM estrellándose contra un helicóptero.<sup>39</sup> En otro vídeo, una ametralladora *Dushka* siria montada encima de un camión pequeño espera con una escuadrilla de MANPADS rebeldes desmontados en una montaña remota, formando un equipo de defensa aérea tipo ametralladora, cohete infrarrojo. En las ciudades, metrajés muestran camiones con *Dushkas* montadas aproximándose a toda velocidad hacia avistamientos de aeronaves como un equipo de defensa aérea improvisado de reacción rápida. Para la primera semana de diciembre, al menos un camión rebelde estaba armado no tan solo con ametralladoras sino también con MANPADS—un vehículo móvil improvisado de “uso general” de artillería de defensa aérea. Además, otros vídeos muestran rebeldes utilizando camuflaje (ramas de árboles cortados y arbustos) y disparando desde puestos encubiertos en huertos y entre edificios. En enero de 2013, un convoy del FAS llevó a cabo una “pasada en revisión” extensa cerca de Aleppo con varios tipos de armamento pesado montados en o remolcados por vehículos militares y civiles capturados.<sup>40</sup>

En particular la marcha hacia el aeropuerto de Damasco conlleva una importancia psicológica y estratégica significativa, demostrando que la sede del poder de al-Assad está en peligro.<sup>41</sup> La presión de los rebeldes en las operaciones del aeropuerto provocaron la cancelación temporal de vuelos hacia la capital siria en las aerolíneas *Emirates Airline* e *Egypt Air* e interrumpió el reabastecimiento de las armas del régimen provenientes de Irán y Rusia. La coacción que ejercieron en el aeropuerto de Damasco, que auspicia el transporte de la milicia siria y las aeronaves VIP, reafirmó los informes de diciembre de al-Assad perdiendo las esperanzas de huir de su país.<sup>42</sup> De hecho, la administración Obama consideró “una intervención más profunda para ayudar a sacar al Presidente Bashar al-Assad del poder”.<sup>43</sup> Tan poco como una semana más tarde, Washington reconoció oficialmente a la nueva Coalición Nacional para las Fuerzas de la Revolución y la Oposición Siria como la autoridad política oficial en Siria. En enero de 2013, a causa de un incre-

mento en los puestos de control rebeldes y temor a ser atacados por SAMs al despegar, más de 80 refugiados rusos viajaron por autobús hacia el aeropuerto de Beirut en el Líbano en lugar de partir desde el aeropuerto internacional en Damasco.<sup>44</sup>

Como se trató anteriormente, los ataques aéreos sirios continuaron aumentando después del fallido cese de fuego Eid al-Adha. Al mismo tiempo, los rebeldes alegaron haber destruido un total de 111 aeronaves sirias, mitad de ellas derribadas en el aire y las otras destruidas mientras estaban estacionadas en la pista.<sup>45</sup> El 12 de diciembre, el régimen lanzó su primer misil *Scud* desde Damasco contra puestos rebeldes en Aleppo, quizás señalando que la guerra civil siria había alcanzado otro hito—esta vez de poderío aéreo a misiles de aire a aire en el teatro a medida que el FSA desgastó la fuerza aérea siria. Hasta la fecha, el régimen sirio ha lanzado más de 25 *Scuds* y misiles “tipo *Scud*” a blancos al norte de Siria y los suburbios en Damasco.<sup>46</sup> El clima en el invierno en Siria verdaderamente ha afectado las operaciones de la fuerza aérea del régimen, pero el uso de misiles pudiese sugerir la presión en la fuerza aérea siria junto con la necesidad de lanzar cada vez más municiones contra los rebeldes que avanzaban y la voluntad de emplear todo armamento disponible en el arsenal del régimen.

Además, el FSA demostró su capacidad de mantener una ofensiva en enero de 2013 cuando los rebeldes se apuntaron su victoria militar más significativa hasta la fecha—la captura de la base aérea estratégica Taftanaz al norte de Siria. Mencionada anteriormente, esta base cerca de Aleppo estuvo bajo ataque durante seis meses. El FSA pudo “concentrar las fuerzas adecuadas, coordinar sus acciones, emplear armamento pesado y sostener el ataque durante meses bajo el ataque aéreo del régimen”.<sup>47</sup> Además, la destrucción de 20 de los helicópteros de la fuerza aérea siria y la captura de grandes cantidades de armamento y municiones, demostró la capacidad de los rebeldes de asediar y capturar bases aéreas fuertemente defendidas.

## Conclusión

La difusión de las protestas a lo largo del Oriente Medio se ha denominado una *Primavera Árabe* pero quizás el término *intifada* describe mejor los acontecimientos en una Siria destruida por la guerra.<sup>48</sup> Hasta ahora, la guerra civil no ha plasmado ni un comienzo nuevo ni un crecimiento nuevo; *intifada*, que significa “lanzar una yema”, parece ser más indicativo de esta lucha contra el régimen.

Si bien la *intifada* siria continúa, algunas conclusiones provisionales se presentan. Durante la guerra, el régimen sirio ha intentado frustrar los planes de los rebeldes con sus sistemas de armamento pesado y, desde el verano el poderío aéreo ha desempeñado un papel crucial. Aeronaves sirias bombardearon zonas pobladas y fuerzas de la oposición, ocasionando la muerte de miles de civiles y por ende permitiéndole al régimen de al-Assad mantener un grado de dominio psicológico. En múltiples discusiones, visitas con los líderes de la oposición y los rebeldes y viajes a la región, el tema emotivo de los bombardeos aéreos dominan las conversaciones.<sup>49</sup> El régimen de Bashar al-Assad algún día se le asociará con el uso de poderío aéreo contra una población civil. Aunque utilizó artillería en mayores cantidades que aeronaves, los sirios consideran que los helicópteros y los aviones de combate son el medio sangriento de la muerte y la destrucción. Por lo tanto, la lucha siria será recordada como otro capítulo oscuro en el expediente de conflictos tales como la Guerra Civil en España y el bombardeo de iraquíes y curdos por parte de Saddam Hussein.

Nadie sabe si el incremento en el uso de poderío aéreo fue una táctica intencionada del régimen o sencillamente surgió de una necesidad para el lanzamiento flexible de municiones. Puede que el régimen se haya resistido a emplear aeronaves por temor a la intervención occidental en la forma de una zona de no vuelo. Presuntamente, al inicio el uso de aeronaves contra civiles hubiese logrado demasiada atención internacional, una lección probablemente aprendida de

los conflictos en Irak, Bosnia y Libia. Mientras que un enfoque paulatino al bombardeo aéreo hizo que la intervención de potencias externas fuese menos probable, los sistemas robustos de defensa aérea sirios, los misiles de superficie a superficie y el inventario de armamento químico más grande influenció a los encargados de formular leyes y a los planificadores militares estadounidenses—un hecho que no pasó desapercibido por otros regímenes totalitarios tales como Corea del Norte e Irán.

El poderío aéreo de al-Assad, aunque sea reducido, conserva la capacidad para atacar en cualquier lugar en Siria en el momento que lo desee. Inclusive una aptitud limitada sigue siendo una herramienta poderosa del régimen para influenciar a los sirios tanto psicológica como físicamente. No obstante, las nuevas tácticas recién adoptadas de ataque y retirada del FSA le han permitido victorias sustanciales a pesar de una campaña aérea implacable, al estilo douhetiano. Finalmente, los rebeldes implementaron una doble estrategia atacando las bases aéreas del régimen e improvisando una red de defensa aérea a baja altitud, evitando una victoria rápida tal como lo predijo Douhet. El régimen sirio y el FSA se han adaptado durante los dos últimos años. La fuerza aérea siria enfrentó una contrainsurgencia inesperada mientras que los rebeldes formaron lentamente un sistema de defensa aérea *ad hoc*, pero eficaz que, combinado con los avances en tierra, a la larga podría terminar la eficacia de las aeronaves y los misiles de superficie de al-Assad.

Queda por ver si el régimen de al-Assad se derrumbará repentinamente o si lentamente se contraerá en un “retazo del estado Alawita” con los triunfos del FSA. Indudablemente, el poderío aéreo le ha permitido al régimen mantenerse en el poder, pero las pérdidas en el campo de batalla y los problemas con el mantenimiento de las aeronaves han paralizado severamente una de las fuerzas aéreas y sistemas de defensa de misiles más grandes en el Oriente Medio. La fuerza aérea siria, aplastada por Israel en 1967 y 1973, se recuperó después de cada derrota con armamento más sofisticado, pero resulta difícil imaginar una supervivencia similar después que termine esta guerra. En vista de la cifra actual de muerte y destrucción, el agotamiento de las reservas de petróleo y una población en crecimiento (con un alto índice de desempleo), uno duda si esa fuerza aérea (históricamente una organización en contra de Estados Unidos) amenazaría a Estados Unidos y sus socios en la región. Los efectos colaterales en Siria crearán una miríada de problemas de seguridad futuros para Estados Unidos, pero serán diferentes a los del modelo antes de 2011 de los escuadrones de combate y defensas aéreas integradas soviéticas encabezadas por un solo líder autócrata.

La falta de participación directa de Estados Unidos en el conflicto justifica más análisis. A medida que la cifra de muertos aumenta, que los grupos islámicos anti Estados Unidos cobran influencia, y a medida que uno considera la expectativa de una falta de control en cuanto a las armas químicas en una Siria después de Assad, los expertos en poderío aéreo discutirán justificadamente lo que Estados Unidos pudo haber hecho, ya sea mediante zonas de no vuelo, ataques aéreos o ayuda con armamento más pesado. Una combinación de la muerte de más de 60.000 civiles, el desplazamiento de millones, y la amenaza “en cualquier momento” de armas químicas eleva la “barra de intervención” futura de Estados Unidos a nuevos niveles. En virtud de los rescates de poderío aéreo en las dos últimas décadas en Irak, Bosnia y Libia, el papel de las fuerzas aéreas occidentales de proteger poblaciones civiles de musulmanes de los gobernantes déspotas evidentemente ha terminado. Por lo tanto la operación Libia antes de Siria puede que se haya convertido en un nota a pié de página en la historia—el último ejemplo de una zona de no vuelo forzada por la Fuerza Aérea de Estados Unidos.

Otros puntos de vista y lecciones aprendidas seguramente saldrán a la superficie a medida que se recibe y se valida más información. El conflicto sirio es verdaderamente demasiado amplio y complejo para que se pueda abarcar en un solo artículo, pero en este se ha tratado de documentar y discutir temas de poderío aéreo a través de un marco histórico de la guerra civil. Las palabras de Douhet y otros que predijeron un terror y temor difundido desde el aire suenan

sorprendentemente ciertos un siglo más tarde. *Guernica* de Picasso—de más de 100 años e inspirada por una guerra, lugar y tiempo diferentes—aún representa la pérdida de vida humana y la destrucción física en la Siria de hoy. Homs, Hama, Aleppo y otras ciudades y aldeas sirias están ligadas a Guernica a través de una narrativa compartida—el poderío aéreo empleado para un fin oscuro y singular. □

#### Notas

1. Jeffrey White, Becado de la Defensa en el *Washington Institute for Near East Policy* (Instituto Washington para Política del Oriente Cercano), y Katie Kiraly, asistente de investigaciones para el Programa sobre Política Árabe, contribuyeron a este artículo.

2. Megan Price, Jeff Klingner y Patrick Ball, *Preliminary Statistical Analysis of Documentation of Killings in the Syrian Arab Republic* (Análisis Estadístico Preliminar de la Documentación sobre Muertes en la República Árabe Siria) (Palo Alto, CA: Benetech, 2 de enero de 2013), 1–4, <http://www.ohchr.org/Documents/Countries/SY/PreliminaryStatAnalysisKillings-InSyria.pdf>.

3. “*Measured Approach to the Syrian Crisis*” (Enfoque medido hacia la crisis siria”, editorial, *New York Times*, 30 de noviembre de 2012, <http://www.nytimes.com/2012/12/01/opinion/a-measured-approach-to-the-syrian-crisis.html>.

4. Robert S. Dudley, “Douhet”, *Air Force Magazine* 94, no. 4 (abril de 2011): 64–67, <http://www.airforce-magazine.com/MagazineArchive/Documents/2011/April%202011/0411douhet.pdf>.

5. Eyal Zisser, *Asad's Legacy: Syria in Transition* (El legado de Assad: Siria en transición) (New York: New York University Press, 2001), 1.

6. Patrick Seale con la ayuda de Maureen McConville, *Asad of Syria: The Struggle for the Middle East* (Assad de Siria: La lucha por el Oriente Medio) (London: I. B. Taurus, 1988), 52. Seale es el biógrafo de Hafiz al-Assad. Una llamada telefónica desde Irak le notificó a los sirios que un avión británico de vigilancia se dirigía desde Irak a lo que despegó de Chipre. “Assad tuvo la satisfacción de dispararle con su cañón”. (ibid.).

7. Ibid., 279.

8. Central Intelligence Agency (Agencia Central de Inteligencia), “Syria”, (Siria) *The World FactBook*, 22 de enero de 2013, <https://www.cia.gov/library/publications/the-world-factbook/geos/sy.html>.

9. Supuestamente, durante una entrevista, Rifaat al-Assad, hermano de Hafiz al-Assad y el comandante en escena en Hama del régimen, disputó la cifra de muertos reportada de 7.000: “¿De qué hablan, 7.0000? No, no. Matamos 38.000”. Thomas L. Friedman, *From Beirut to Jerusalem* (De Beirut a Jerusalén) (New York: Farrar, Straus, Giroux, 1989), 90. Este libro que todos deben leer ganó el Premio Nacional al Libro en 1989.

10. Ibid., 91.

11. “*We Can't Win Media War with West but It's Not Battle That Counts*” (No podemos ganar la guerra de los medios de comunicación con occidente pero no es la batalla lo que cuenta), Organización Autónoma sin fines de Lucro (“TV-Novosti”), 17 de mayo de 2012, <http://rt.com/news/syria-media-battle-assad-429/>. Al-Assad descrito repetidamente al FSA como “un grupo de criminales convictos, compuesto entre otras cosas de fanáticos religiosos tipo al-Qaeda, extremistas y terroristas y hasta cierto punto de mercenarios extranjeros, predominantemente de otros estados árabes” (ibid.) Algunos miembros del FSA son, de hecho, islamistas extremistas, pero la gran mayoría no están afiliados con al-Qaeda.

12. Friedman, *From Beirut to Jerusalem*, 91. De forma escalofriante, Friedman trae a colación este punto durante la rebelión de la Hermandad Musulmana décadas antes. Esta premisa es aún más recalcada hoy a través de la aceptación indiferente del FSA por algunas facciones suní, curdas y cristianas. Durante la “Primavera Árabe” y otros tiempos en la historia del Oriente Medio, cuando se derrota un régimen autócrata, los grupos minoritarios tienden a estar en riesgo—por ejemplo, analicen la situación apremiante reciente de los cristianos coptos en Egipto.

13. Thomas Hobbes (1588–1679) fue un filósofo inglés y teórico político mejor conocido por su libro *Leviathan* (Leviatán) (1651), en el que alega que uno puede asegurar la sociedad civil solamente a través de la sumisión universal a la autoridad absoluta de una soberanía.

14. *Wikipedia: The Free Encyclopedia* (Wikipedia: La Enciclopedia Libre), s.v. “*Timeline of the Syrian Civil War (January–April 2011)*” (Cronología de la Guerra Civil Siria [enero a abril de 2011]) [ver “6 de marzo”], [http://en.wikipedia.org/wiki/Timeline\\_of\\_the\\_Syrian\\_civil\\_war\\_\(January%20%80%93April\\_2011\)#15\\_March\\_E2.80.93\\_22Day\\_of\\_Rage.22](http://en.wikipedia.org/wiki/Timeline_of_the_Syrian_civil_war_(January%20%80%93April_2011)#15_March_E2.80.93_22Day_of_Rage.22). Para un vídeo del Día de la Ira, ver “*Syrian Revolution, Syria*” (Revolución siria, Siria), vídeo en YouTube, 15 de marzo de 2011, <https://www.youtube.com/watch?v=75Ng0J6DdH0>.

15. Anne Sinai y Allen Pollack, editores, *The Syrian Arab Republic: A Handbook* (La República Árabe Siria: Un manual) (New York: American Academic Association for Peace in the Middle East, 1976), 59.

16. Durante la Primera Guerra Mundial, Deraa—una intersección vital de los ferrocarriles Jerusalén-Haifa-Damasco-Medina—fue la escena de la tortura de los turcos otomanos de T. E. Lawrence, conocido también como *Lawrence of Arabia* (Lorenzo de Arabia). T. E. Lawrence, *The Seven Pillars of Wisdom* (Los siete pilares de la sabiduría) (New York: G. H. Doran, 1926).

17. La ruta de Aleppo a Damasco no es ajena al conflicto y la miseria musulmana. La división entre los chiítas y sunitas fue personificada en la batalla de Karbala (680 CE) en lo que hoy es Ira, donde el nieto de Muhammad, Imam Hus-

sein, y 70 seguidores fueron asesinados por Yazid I, un gobernante basado en Damasco. El aniversario de la derrota hoy se conoce como “Ashur”, un día sagrado de ayuno y oraciones, en el que los chiítas conmemoran el abandono percibido de Hussein y sus seguidores. Yazid, un sunita tradicional, ordenó que los sobrevivientes capturados de Karbala, junto con la cabeza de Hussein, fuesen exhibidos en la región. Después de una breve parada en Mosul, la procesión viajó hacia Aleppo, al sur de Homs, y finalmente terminó en Damasco. Consultar Andrew Tabler, *In the Lion's Den: An Eyewitness Account of Washington's Battle with Syria* (En la cueva del león: Recuento de la batalla de Washington con Siria) (Chicago: Lawrence Hill Books, 2011), 170.

18. Dr. Radwan Ziadeh, “The Battle for Syria” (La batalla por Siria), (charla, *School of Advanced International Studies* (Escuela de Estudios Avanzados Internacionales), Johns Hopkins University, 30 de noviembre de 2012), <http://mms.tv.eyes.com/Transcript.asp?StationID=200&Date=12%2F3%2F2012+12%3A21%3A12+PM&Term=washington+institute+for+near+east+policy&PlayClip=TRUE>.

19. Joseph Holliday y Christopher Harmer, *Syrian Air Force and Defense Overview* (Resumen de la Fuerza Aérea y Defensa Siria) (Washington, DC: *Institute for the Study of War* (Instituto para el Estudio de la Guerra), 25 de octubre de 2012), <http://www.understandingwar.org/press-media/graphsandstat/syrian-air-force-air-defense-overview>. El Sr. Holliday, un ex capitán de inteligencia del Ejército de EE.UU. con gran experiencia en el Oriente Medio, es un analista en el Instituto para el Estudio de la Guerra—una organización independiente sin fines de lucro dedicada a la investigación pública. Una de las primeras personas en documentar y darle seguimiento al uso del poderío aéreo sirio contra civiles, el Sr. Holliday fundó y encabeza un grupo interinstitucional para la solución de problemas compuesto de diplomáticos, militares, de la comunidad de inteligencia y de expertos sirios.

20. Eddie Boxx y Jeff White, “Responding to Assad's Use of Airpower in Syria” (Respondiendo al uso de poderío aéreo de Assad en Siria), *Policywatch* 1999, *Washington Institute for Near East Policy*, 20 de noviembre de 2012, <http://www.washingtoninstitute.org/policy-analysis/view/responding-to-assads-use-of-airpower-in-syria>.

21. *Ibid.*

22. David Axe, “Danish Architect Maps Every Plane, Helicopter Shot Down by Syrian Rebels” (Arquitecto danés traza cada aeronave, helicóptero derribado por rebeldes sirios), *Wired*, 19 de octubre de 2012, <http://www.wired.com/dangerroom/2012/10/mapping-syrian-air-war>.

23. Información obtenida a través de vídeos *YouTube*. A pesar de que estos hechos no se pueden verificar independientemente, el autor estableció un enlace entre los enfrentamientos y ataques de esas aeronaves a las bases aéreas.

24. Jeffrey White, “Syria's Internal War Turns against the Regime” (La guerra interna de Siria se torna contra el régimen), *Policywatch* 1996, *Washington Institute for Near East Policy*, 13 de noviembre de 2013, <http://www.washingtoninstitute.org/policy-analysis/view/syrias-internal-war-turns-against-the-regime>.

25. Anne Barnard, “As Killings Go On, Syria Reacts Strongly to War-Crimes Petition” (A medida que continúan los asesinatos, Siria reacciona con fuerza a petición de crímenes de guerra), *New York Times*, 19 de enero de 2013, [http://www.nytimes.com/2013/01/20/world/middleeast/syria-war-developments.html?ref=syria&\\_r=0](http://www.nytimes.com/2013/01/20/world/middleeast/syria-war-developments.html?ref=syria&_r=0).

26. Además de la cobertura convencional de los medios de comunicación, vides de *YouTube* subidos por el régimen y las fuerzas rebeldes al igual que informes anti Assad por el Observatorio Sirio para los Derechos Humanos, con sede en Gran Bretaña, los comités locales de coordinación y las organizaciones no gubernamentales proporcionaron documentación extensa de los acontecimientos a medida que ocurrían.

27. *Forum*, Brookings Institution, subject: “Syria: The Path Ahead” (Siria: El camino por delante), 8 de noviembre de 2012. Mike Doran, el *Roger Hertog Senior Fellow* en el Centro Saban para Política en el Oriente Medio en Brookings y Salman Shaikh, director del Centro Doha en Brookings, compartieron sus puntos de vista durante el foro. El artículo reciente de Shaikh *Losing Syria (and How to Avoid It)* (Perdiendo a Siria, y cómo evitarlo) fue el centro de la discusión, moderada por Daniel L. Byman, Becado Superior y Director de Investigaciones Centro Saban para la Política en el Oriente Medio.

28. Estos hallazgos fueron presentados y adoptados el 12 de octubre de 2012, en el grupo de trabajo del Proyecto Sirio auspiciada por el Instituto para el Estudio de la Guerra (ISW, por sus siglas en inglés) y presidido por Joseph Holliday. El panel constaba de grupos pro derechos humanos, organizaciones no gubernamentales, personal del Departamento de Estado, Departamento de Defensa, la comunidad de inteligencia, grupo de expertos sirios, y empleados del Congreso. La información fue proporcionada de dos fuentes—vídeos *YouTube* de los ataques aéreos y el Observatorio Sirio para los Derechos Humanos. Las gráficas muestran aeronaves de ala giratoria en lugar de ala fija. El “tamaño del recipiente” es un día (cada barra representa un día) y los datos no representan la hora del día—solamente el periodo de 24 horas durante el cual ocurrió un ataque aéreo. Los ejemplos que el ISW identificó como aeronaves contra emplazamientos de rebeldes proviene del siguiente análisis: Si el combate terrestre ocurrió entre los rebeldes y las fuerzas del régimen en el mismo lugar y en la misma fecha que los ataques aéreos, entonces éstos atacaron directamente a los rebeldes. Si no hubo ninguna actividad por parte del FSA, y si los ataques aéreos fueron corroborados por otras fuentes, entonces los civiles fueron los blancos objetivos. Por supuesto, no todo ataque aéreo que hirió a civiles fue intencional, el régimen carecía de municiones guiadas por precisión y de datos actualizados de selección de blancos. Pero al analizar los vídeos publicados por el régimen y otras evidencias, uno podría concluir razonablemente que libró una campaña contra civiles. Para más información y más datos sobre los ataques aéreos, consultar Holliday y Hammer, *Syrian Air Force and Defense Overview*.

29. Oliver Homes y Shaimaa Fayed, “*Syria Undecided on Ceasefire Proposal, Rebels Divided*” (Siria indecisa sobre propuesta de cese de fuego, rebeldes divididos), Reuters, 24 de octubre de 2012, <http://www.reuters.com/article/2012/10/24/us-syria-crisis-idUSBRE88J0X720121024>.

30. Holliday y Harmer, *Syrian Air Force and Defense Overview*, problemas de *Scramble*, consultado el 1º de febrero de 2013, <http://www.scramble.nl/sy.htm>; e Instituto Internacional para Estudios Estratégicos, *The Military Balance 2011* (El balance militar 2011), (Washington, DC: International Institute for Strategic Studies, 2011), 331.

31. “*Syrian Colonel ‘Defects’ in Jet to Jordan*” (Coronel sirio deserta en jet a Jordania), *Guardian*, 21 de junio de 2012, <http://www.guardian.co.uk/world/middle-east-live/2012/jun/21/egypt-election-result-delay-coup-live>.

32. “*Russia Will Not Deliver Yak-130 Fighter Jets to Syria*” (Rusia no entregará aviones de combate Yak-130 a Siria), *Airforce-technology.com*, 9 de julio de 2012, <http://www.airforce-technology.com/news/newsrussia-syria-fighter-jet-delivery>.

33. Jeff White, Washington Institute for Near East Policy, entrevista por el autor, 29 de noviembre de 2012 (opinión de un experto basada en un vídeo *YouTube* de Fitter, publicada el 16 de noviembre de 2012. [http://www.youtube.com/watch?v=n5f5mjjpVSEk&feature=player\\_embedded](http://www.youtube.com/watch?v=n5f5mjjpVSEk&feature=player_embedded)).

34. Boxx y White, “*Assad’s Use of Airpower.*”

35. *Ibid.*

36. “*FSA Targeting al-Assad Regime Air Bases—Sources*” (FSA ataca bases aéreas y abastos), *Asharq Alawsat*, 7 de diciembre de 2012, <http://www.asharq-e.com/news.asp?section=1&id=32082>.

37. Boxx y White, “*Assad’s Use of Airpower.*”

38. Joby Warrick, “*Missiles Boost Rebels’ Arsenal*” (Misiles realzan arsenal de rebeldes), *Washington Post*, 29 de noviembre de 2012, A1, <http://thewashingtonpostnie.newspaperdirect.com/epaper/viewer.aspx>.

39. Babak Dehghanpisheh, “*Syrian Rebels Take Two Military Bases in Heavy Fighting*” (Rebeldes sirios se apoderan de dos bases militares durante intensos enfrentamientos), *Washington Post*, 28 de noviembre de 2012, 13, [http://articles.washingtonpost.com/2012-11-27/world/35509205\\_1\\_syrian-rebels-military-bases-aleppo](http://articles.washingtonpost.com/2012-11-27/world/35509205_1_syrian-rebels-military-bases-aleppo).

40. Vídeo *YouTube*, publicado el 16 de enero de 2013, [http://www.youtube.com/watch?feature=player\\_embedded&v=y5jsI739NRw](http://www.youtube.com/watch?feature=player_embedded&v=y5jsI739NRw).

41. La captura del aeropuerto de Damasco, el más transitado en el país y un centro importante en la región, tendría gran significado. En Damasco aterrizan más de 40 aerolíneas de pasajeros y de carga provenientes del Oriente Medio, Europa, África, y la Mancomunidad de Estados Independientes, con un promedio de más de 4,5 millones de pasajeros al año. Desde la Segunda Guerra Mundial, las fuerzas estadounidenses han presenciado el valor estratégico de apoderarse de aeropuertos. Por ejemplo, la captura por parte de la 3ª División de Infantería del Aeropuerto Internacional de Bagdad en el 2003 le envió una señal al mundo que Estados Unidos había ganado la contienda táctica para la ciudad.

42. Jeffrey White, “*Last Act in Damascus*” (El último acto en Damasco), Washington Institute for Near East Policy, 11 de diciembre de 2012, <http://www.washingtoninstitute.org/policy-analysis/view/last-act-in-damascus>.

43. David E. Sanger y Eric Schmitt, “*U.S. Weighs Bolder Effort to Intervene in Syria’s Conflict*” (Estados Unidos considera iniciativa decisiva para intervenir en el conflicto de Siria), (*New York Times*, 28 de noviembre 2012, 1, [http://www.nytimes.com/2012/11/29/world/us-is-weighing-stronger-action-in-syrian-conflict.html?\\_r=0](http://www.nytimes.com/2012/11/29/world/us-is-weighing-stronger-action-in-syrian-conflict.html?_r=0)).

44. “*Russians Flee Syrian Conflict on Planes from Beirut*” (Rusos huyen del conflicto sirio en aviones de Beirut), BBC, 22 de enero de 2013, <http://www.bbc.co.uk/news/world-middle-east-21140041>.

45. Bassel Oudat, “*Airport Battles in Syria*” (Batallas en el aeropuerto en Siria), *Al-Ahram Weekly*, 6 December 2012, <http://weekly.ahram.org.eg/News/497/19/Airport-battles-in-Syria.aspx>. Durante el conflicto, inclusive con metrajés documentados de vídeos, ha sido difícil verificar el número de aeronaves derribadas. Sin embargo, los vídeos sugieren que 100 parece una cifra realista del total de aeronaves sirias dañadas en combate.

46. Como parte del Proyecto de la Base de Datos de Misiles Sirios en el Washington Institute for Near East Policy, a diario un equipo investiga vídeos en *YouTube* y de otros medios de comunicación publicados por el FSA y la fuerza aérea siria para lanzamientos de *Scud* u otros misiles de superficie a superficie. A menudo los informes de los medios de comunicación utilizan el término *Scud* para describir todos los misiles de superficie, por lo tanto la meta es definir el tipo exacto de misil empleado. La información documentada incluye tipo de lanzador, cantidad de lanzamientos, origen del lanzamiento, ubicación de blanco, tipo de misil y tipo de blanco. Con la ayuda del meteorólogo, Capitán (USAF) Brian Yates, el equipo analiza los lanzamientos de misiles en el contexto del clima sirio para identificar si las fuerzas del régimen emplean misiles en lugar de aeronaves cuando hay mal tiempo o si los emplean en desespero. En este momento no hay suficientes datos completos para formular una conclusión; por lo tanto, el proyecto de investigación está en curso. Utilizando vídeos *YouTube* de los ataques de misiles, el Washington Institute for Near East Policy ha identificado y registrado tentativamente los ataques de misiles. En ellos se observa que los *Scuds* son transportados en vehículos lanzadores con llantas y lanzados verticalmente (por lo regular de color blanco y grandes) con humo significativo antes del lanzamiento (quizás a causa del propulsante líquido) —básicamente cohetes nazis V-2 de 1944 mejorados. En contraste los Fateh 100 son de un color más oscuro (café claro o verde olivo) que los misiles *Scud* y son básicamente cohetes sobre lanzadores con llantas y sistema de rieles SA-2. Por lo tanto tienen que lanzarse a un ángulo pronunciado (observe que el riel permanece después de lanzarse el misil), muy parecido a los “cohetes de botella” grandes. El SS-21 es también un misil que no es blanco transportado en un vehículo lanzador de seis llantas, pero no deja el riel detrás después de ser lanzado y poco después se coloca en posición vertical.

47. Andrew J. Tabler, Jeffrey White y Aaron Y. Zelin, “*Fallout from the Fall of Taftanaz*”, (Los efectos secundarios de la derrota de Taftanaz), *Policywatch* 2015, Washington Institute for Near East Policy, 14 de enero de 2013, <http://www.washingtoninstitute.org/policy-analysis/view/fallout-from-the-fall-of-taftanaz>.

48. Durante los últimos 20 años, el Dr. Robert Satloff, director del Washington Institute for Near East Policy, ha explicado en múltiples ocasiones el término equivocada de una *Primavera Árabe* y por qué el término árabe *intifada* representa mejor las tensiones en el Oriente Medio. Estoy muy endeudado con sus amplios conocimientos de la región y su disponibilidad para explicar una zona muy complicada, pero importante, del mundo.

49. Mediante las iniciativas del Washington Institute for Near East Policy y el apoyo del experto en Siria, Andrew Tabler, (autor del *In the Lion’s Den* [ver nota 17], otro libro acerca de Siria que todos deben leer) el autor ha logrado una perspicacia significativa en la oposición al reunirse con líderes sirios de la oposición y un miembro del FSA (por motivos de seguridad los nombres de la oposición se han revelado).



**El Teniente Coronel S. Edward Boxx**, USAF (BA, University of Texas en El Paso; MS, Embry-Riddle University; MA, Air University) es becado visitante de la Defensa en el Washington Institute for Near East Policy. Anteriormente, dirigió el Elemento de Coordinación del Componente Aéreo (ACCE, por sus siglas en inglés) para la Fuerza de Tarea Conjunta Interinstitucional Sur (JIATFS, por sus siglas en inglés), Cayo Hueso, Florida, donde estuvo a cargo de integrar los recursos de la Fuerza Aérea para contrarrestar las operaciones de contrabando aéreas y marítimas. Un veterano administrador de batalla de combate aéreo, ha sido calificado en el AWACS E-3, y el Joint STARS E-8. El Coronel Boxx cuenta con 1.500 horas de combate y apoyo de combate en apoyo a operaciones aéreas en Yemen, Turquía, Arabia Saudí, Irak y Afganistán. Mientras estuvo desplegado en el 2006 en apoyo a la Operación Libertad para Irak, participó en operaciones para contrarrestar el contrabando y empleo de dispositivos explosivos improvisados (IED, por sus siglas en inglés). Además voló misiones en apoyo a las zonas de no vuelo al norte y sur en Irak durante la década de los años noventa. El Coronel Boxx es egresado de la Escuela Superior para Oficiales y de la Escuela Superior de Comando y Estado Mayor, y ha publicado varios artículos sobre poderío aéreo.

# Seguridad de las Computadoras

## ¿El Talón de Aquiles de la Fuerza Aérea Electrónica?\*

TENIENTE CORONEL ROGER R. SCHELL, USAF

El oficial de la KGB se dirigió al grupo selecto de oficiales soviéticos con el acostumbrado tono secreto pero con un aire de excitación inusual:

Camaradas, hoy les hablaré de uno de los descubrimientos más significativos de recopilación de inteligencia desde que se “descifraron” los códigos “indescifrables” japonés y alemán en la SGM—la penetración de la seguridad de las computadoras estadounidenses. Prácticamente (incluso literalmente) no hay ningún secreto importante de defensa nacional de EE.UU. que no esté guardado en una computadora, en algún lugar. Al mismo tiempo, hay pocas computadoras (de haberlas) en su sistema de defensa nacional que no sean accesibles en teoría, e incluso en la práctica, a nuestra curiosidad. Y lo que es aún mejor, no tenemos que esperar a que envíen esa información particular que deseamos para que podamos interceptarla; podemos solicitar y obtener materiales de interés específicos para nosotros, sin prácticamente ningún riesgo para nuestros agentes.

Los estadounidenses han desarrollado una tecnología de “núcleo de seguridad” para resolver su problema, pero no necesitamos preocuparnos—recientemente discontinuaron el trabajo en esta tecnología. Son conscientes del potencial de un problema de seguridad informático, pero con su descuido habitual decidieron no corregir el problema hasta que se verificaran ejemplos de nuestra explotación activa. Nosotros, por supuesto, no les debemos dejar encontrar estos ejemplos.

Su primera reacción a esta situación puede ser, “¡absurdo!” Pero antes de rechazarla de inmediato, reconozcamos que sabemos que puede pasar. La pregunta es la siguiente: ¿aplicaremos una tecnología y una política firmes antes de que ocurra esto? Para asegurarnos de ello, hay cosas que no sabemos sobre la probabilidad de éxito de un esfuerzo de ese tipo, pero podemos evaluar racionalmente los factores de control más sobresalientes:

- La gran *vulnerabilidad* de las computadoras contemporáneas se ha indicado claramente en la experiencia del autor con una penetración sin detectar mecanismos de seguridad. Además, las debilidades de seguridad están documentadas en informes militares y civiles.
- La *capacidad* de los soviéticos (o de cualquier grupo hostil importante) para lograr la penetración requerida es bastante evidente. De hecho, no se requieren destrezas particulares más allá de las de los profesionales informáticos normalmente competentes.
- La *motivación* de dicha actividad de recopilación de información es aparente evidentemente a primera vista. Con frecuencia se informa del gran alcance y de la gran intensidad de los esfuerzos de inteligencia soviéticos en áreas como la interceptación de comunicaciones.
- El *daño* potencial de la penetración aumenta con la cada vez mayor penetración de información sensible en computadoras y la interconexión de estas computadoras en redes grandes. Mediante la penetración en computadoras un enemigo podría, por ejemplo, arriesgar planes de empleo de aviones caza tácticos o arriesgar planes de operación y determinar objetivos para misiles nucleares.
- La *oportunidad* de una explotación hostil de estas vulnerabilidades está aumentando cada vez más debido al mayor uso de computadoras y a la falta de una política de seguridad significativa que controle su uso. En nombre de la eficiencia se permite a muchas más perso-

---

\*Reprinted from *Air University Review* 30, no. 2 (January–February 1979): 16–33.

nas con menos (o ninguna) autorización un acceso más sencillos a los sistemas de computadoras clasificados.

Tenemos un problema y una solución a mano. El examen detallado de la capacidad y motivación de una nación hostil (por ejemplo, Unión Soviética) en esas áreas está debidamente en el campo del analista de inteligencia y en gran medida fuera del alcance de este artículo. No obstante, trazará los límites del problema de seguridad de la computadora y mostrará cómo el método del núcleo de seguridad cumple los requisitos para una solución factible—aunque la terminación reciente ha cortado de raíz un trabajo muy prometedor hacia una solución.

## ¿Qué es lo que hace que las computadoras sean un problema de seguridad?

Aunque es necesaria una cierta apreciación de sutileza para entender los detalles del problema de seguridad informática, nuestro objetivo aquí es iluminar los temas básicos fundamentales. Para entender estos temas, examinaré no solamente las capacidades y limitaciones de las computadoras mismas sino también sus usos.

En primer lugar, damos por sentada la necesidad fundamental de proteger debidamente contra los riesgos la información militar sensible clasificada. Desde hace mucho tiempo, se ha reconocido la seguridad como uno de los principios bélicos básicos, y a través de la historia, la seguridad o su falta han sido un factor importante en el resultado de batallas y guerras. Podemos y controlamos estrictamente la información cuando la diseminación es teórica. Por lo tanto, no es lógico hacer caso omiso del hecho de que las computadoras puede diseminar la misma información a cualquiera que sepa cómo pedirla, omitiendo completamente los costosos controles que ponemos en la circulación de documentos.

En segundo lugar, debemos apreciar que la “explotación del crecimiento fenomenal de las ciencias informáticas es un área importante de énfasis tecnológico dentro del DoD”.<sup>1</sup> Actualmente, carecemos de una superioridad cuantitativa (o incluso paridad) en varias áreas de niveles de fuerzas, y las computadoras parecen proporcionar la superioridad cualitativa que debemos tener. La necesidad de estas capacidades es clara cuando nos damos cuenta de que las buenas capacidades “C<sup>3</sup> [comando, control y comunicaciones] pueden duplicar o triplicar la eficacia de la fuerza; por el contrario, una C<sup>3</sup> ineficaz ciertamente pone en peligro o niega el objetivo buscado”.<sup>2</sup> De hecho, nos hemos convertido en un sentido muy real en una “Fuerza Aérea electrónica”<sup>3</sup> con computadoras como base.

Por último, necesitamos reconocer que algunas vulnerabilidades importantes pueden acompañar a las ventajas sustanciales de la tecnología informática. La mayoría de las personas que toman decisiones no pueden permitirse el tiempo de mantener un entendimiento completo de una tecnología informática que se desarrolla de forma muy veloz. Pero aún menos pueden permitirse el lujo de ignorar lo que la computadora puede hacer y también sobre cómo puede fallar. En particular, un comandante responsable de la seguridad debe asegurarse de que los controles de diseminación se extiendan a las computadoras. Debe poder hacer las preguntas siguientes—para hacer aflorar la vulnerabilidad potencial para efectuar un examen crítico y sin sesgo.

### *Lecciones históricas en tecnología de emergencia*

No es nuevo encontrar que una tecnología emergente tiene sus ventajas y desventajas. En particular, la amenaza a la que se enfrentan las computadoras se ilustra hoy en la evolución de las comunicaciones eléctricas militares—una tecnología revolucionaria anterior. Nuestro riesgo de seguridad de comunicaciones del Eje fue fundamental para el desenlace de la SGM, y las com-

putadoras ofrecen ahora a nuestros enemigos la oportunidad de dar un giro de 180 grados a la situación.

Los especialistas de comunicaciones militares reconocieron pronto la vulnerabilidad de la transmisión eléctrica a la interceptación, por ejemplo, mediante micrófonos ocultos o escuchas clandestinas de señales de radio. Las soluciones fueron sencillas y efectivas pero drásticas: restringir la transmisión solamente a información relativamente poco importante (es decir, sin clasificar) o rutas de transmisión vigiladas físicamente y protegidas contra la intrusión. Igualmente, durante varios años, la Fuerza Aérea restringió el uso de computadoras a datos sin clasificar o a una computadora protegida especializada en usuarios autorizados (aprobados). En ambos casos, las soluciones de seguridad limitaron el uso de la tecnología donde más se necesitaba: para obtener información importante en situaciones potencialmente hostiles, como asistencia en el campo de batalla.

Las restricciones de seguridad de comunicaciones dieron lugar a diversos dispositivos criptográficos. Estos dispositivos iban a codificar información en una forma ininteligible y por tanto sin clasificar de modo que no se requería la protección de toda la ruta de transmisión. No obstante (de importancia suprema para nosotros aquí) esto cambió dramáticamente la propia naturaleza del problema de seguridad propio: desde una cuestión de protección física a una pregunta de eficacia técnica. Se discutió la eficacia de los dispositivos criptográficos, basada no en un análisis técnico cuidadoso sino en una ausencia aparente de una forma conocida para contrarrestarlos. En el presente, la tecnología informática está en una posición análoga con un argumento similar por su eficacia contra el acceso no autorizado a datos informáticos. En ambos casos, los argumentos parecen ofrecer un riesgo aceptable a pesar de tener una base técnica de hecho débil.

Los dispositivos criptográficos técnicamente débiles encontraron un uso militar amplio debido a la falsa confianza y a la urgente necesidad operacional de las comunicaciones eléctricas. Un ejemplo notable fue la máquina Enigma usada por los alemanes durante la SGM. Su red de mando y control nacional de alto nivel usada para la seguridad de comunicaciones durante la guerra. Como indica *el secreto Ultra*, “los alemanes consideraban que su código era completamente seguro”.<sup>4</sup> No obstante, antes de que empezara realmente la guerra, los británicos habían “resuelto de hecho el rompecabezas de Enigma”.<sup>5</sup> La Fuerza Aérea está desarrollando una dependencia similar con cada decisión (formal o de hecho) para acreditar controles de seguridad informáticos. En cualquier caso, las decisiones políticas permiten que una debilidad técnica se convierta en una vulnerabilidad militar.

Los ejemplos durante la SGM muestran cómo la tendencia a defender decisiones anteriores (aceptar y usar técnicas más plausibles) aseguran al enemigo disponer de oportunidades de explotación. En Europa las señales descifradas de Enigma (llamadas Ultra) “no solo daban la fuerza completa y la disposición del enemigo, sino que mostró que los aliados [sus tropas] podían lograr una sorpresa táctica”.<sup>6</sup> De hecho, el General Dwight Eisenhower afirmó que “Ultra fue decisivo”.<sup>7</sup> El libro titulado *The Codebreakers (Los descifradores)* describe una confianza similar equivocada de los japoneses y observa que los criptoanalistas estadounidenses “contribuyeron enormemente a la derrota del enemigo, acortaron considerablemente la guerra y salvaron muchos miles de vidas”.<sup>8</sup> Desde luego, los alemanes “deben haberse sorprendido por nuestros conocimientos de las posiciones de sus submarinos, pero afortunadamente no aceptaron el hecho de que habíamos descifrado Enigma”.<sup>9</sup> De forma similar, los japoneses “estaban hipnotizados con la ilusión de que sus códigos nunca corrieron un riesgo serio”.<sup>10</sup> Parece que las autoridades del Eje no reconocían su debilidad de seguridad sin la confirmación directa de la contrainteligencia—y esto solo salió a la luz después de que perdieran la guerra. En lo que se refiere a la seguridad informática de la Fuerza Aérea, la ausencia de guerra ha excluido su explotación definitiva; sin embargo, la falta de contrainteligencia firme en la explotación ya se ha ofrecido como evidencia de seguridad efectiva.

Aunque los esfuerzos técnicos llevaron a estas vulnerabilidades devastadoras, fueron sin embargo expertos técnicos como William Friedman los que proporcionaron una base técnica firme: “Sus estudios teóricos, que revolucionaron la ciencia, fueron correspondidos por sus soluciones reales, que la asombraron [la comunidad científica].”<sup>11</sup> Hoy, nuestras fuerzas armadas hacen un uso amplio de dispositivos criptográficos con confianza. Para las computadoras, al igual que para las comunicaciones, el quid de la cuestión es la eficacia del mecanismo de seguridad. El trabajo riguroso lógicamente reciente ha producido una tecnología de núcleo de seguridad. No obstante, el DOD no está aplicando aún esta tecnología.

El empuje de esta revisión histórica se recoge en la máxima, “Aquellas personas que no pueden recordar el pasado están condenadas a repetirlo”. Los paralelos históricos se resumen en la Tabla I. La lección principal que hay que aprender es esta: no confíe la seguridad a la tecnología a menos que la tecnología sea demostrablemente fiable, y la ausencia de riesgo demostrada no es absolutamente una demostración de seguridad.

<b>Comunicaciones eléctricas</b>		<b>Computadoras electrónicas</b>
	Uso limitado	
rutas protegidas solo sin clasificar		instalación especial solo sin clasificar
	Seguridad plausible	
tecnología criptográfica crucial para la seguridad sin contrainteligencia conocida base técnica débil		seguridad interna controles cruciales sin penetración conocida base técnica débil
	Dependencia in justificar	
confianza falsa en la criptografía aceptación política		confianza falsa en controles internos aceptación política
	Enemigo subestimado	
intercepción repetida y sin detectar los defensores exigen contrainteligencia		acceso repetido, sin detectar y selectivo los defensores exigen contrainteligencia
	Tecnología adecuada	
teoría de información		núcleo de seguridad

**Tabla I. Evolución comparativa de los problemas de seguridad**

*Distinción entre cálculo y protección*

La computadora dada de una instalación puede procesar datos sensibles de forma segura, y una máquina idéntica puede ser totalmente insegura en otra instalación. La clave para entender el problema de seguridad informático es distinguir cuándo la computadora solamente calcula y cuando debe proporcionar también seguridad. Estos son dos casos muy distintos.

En el primer caso, llamada comúnmente “modalidad especial”, la computadora y todos sus usuarios están dentro de un solo perímetro de seguridad establecido por guardas, perros, cercas, etc. Mediante el uso de comunicaciones seguras, este perímetro puede ampliarse geográficamente a terminales remotas. Solamente se requieren estos controles de seguridad externos para mantener la seguridad del sistema. El uso de la computadora está restringido de modo que en cualquier momento todos los usuarios, remotos o locales, son un acceso autorizado a todos los datos informáticos. Un atacante potencial debe sortear los controles externos y penetrar en el círculo del personal autorizado. La computadora solo calcula; ningún fracaso ni subversión de la computadora misma puede poner en riesgo la seguridad debido al entorno protegido.

En el segundo caso, llamado comúnmente “modalidad de niveles múltiples”, la computadora misma debe distinguir internamente múltiples niveles de sensibilidad de información y autorización del usuario. En particular, la computadora debe proteger cierta información de ciertos usuarios. Para la modalidad de múltiples niveles, los controles de seguridad internos de equipos y programas de computadoras deben asegurarse de que cada usuario pueda tener acceso solo a la información autorizada. Para la seguridad de niveles múltiples, la computadora misma debe proteger claramente así como calcular. Para el atacante potencial, simplemente bastará obtener acceso a los usuarios periféricos de la computadora—si se puede penetrar en los controles internos.

Los controles de seguridad de múltiples niveles funcionan de forma análoga a un dispositivo criptográfico; su eficacia es esencial para la seguridad de la información. Debido a la estructura inherente de las computadoras, una debilidad de seguridad de múltiples niveles invita a una explotación repetida. Además, esas fallas de seguridad interna de la computadora casi nunca se detectan. Contrariamente a las comunicaciones donde el acceso del enemigo al tráfico importante es un asunto de probabilidad, en una computadora penetrada se tiene un acceso selectivo, no solamente para la extracción sino también para la modificación de información a su elección. Lo que es peor, el poder de procesamiento de las computadoras modernas proporciona esta información de modo rápido y completo.

Si estamos preocupados por la protección de nuestros códigos criptográficos, entonces ciertamente no tiene sentido abandonar nuestras computadoras. Debemos darnos cuenta de que la modalidad de múltiples niveles puede ayudar al atacante a menos que los controles internos de la computadora misma proporcionen una protección fiable.

### *Evidencia de controles de seguridad débiles*

La cuestión crítica entonces es esta: ¿nos atrevemos a confiar en los controles de seguridad interna de programas de computadora y hardware? La experiencia del autor con debilidades de seguridad indica que las computadoras contemporáneas no proporcionan una protección fiable. Se comprobaron las computadoras propuestas como suficientemente seguras para proteger información sensible en caso de deficiencias de seguridad. Un equipo de expertos técnicos sancionado formalmente vio debilidad en estas computadoras supuestamente seguras. (Para mayor precisión, los ejemplos se limitarán a esas evaluaciones en las que el autor participó personalmente).

El equipo de expertos técnicos operó como un usuario legítimo con acceso limitado a una pequeña parte de la información en el sistema. El objetivo del equipo era penetrar en los controles de seguridad internos y demostrar que se podría obtener el acceso no autorizado. En todos los casos de la experiencia del autor, se descubrieron debilidades de seguridad graves después de solo unas cuantas horas o días de esfuerzo.

*Contraseñas para pedir.* Un elemento común de protección es una contraseña o clave secretas que el usuario debe proporcionar para recibir servicios o información. Para ser efectiva, el secreto de las contraseñas debe conservarse. Una computadora IBM 370 con la opción de reparto de tiempo (TSO) tenía terminales remotas en diversas áreas descontroladas; las contraseñas se-

cretas restringían el acceso del usuario. Esta computadora particular contenía información sensible de selección de fuentes de adquisición de la Fuerza Aérea con una diseminación muy controlada. Los miembros del equipo de expertos técnicos averiguaron que meramente tenían que preguntar por nombre el archivo de las contraseñas para que imprimieran las contraseñas de todos los usuarios de TSO—sin traza de que habían corrido riesgo. Los diseñadores no se habían fijado en la relación entre la seguridad y la capacidad para imprimir un archivo.

*La buena publicidad no es suficiente.* En el Pentágono, un sistema de General Electric llamado “GCOS” proporcionó un cálculo clasificado (secreto) para el Estado Mayor del Aire y otros con terminales remotas protegidas en lugares seleccionados. El fabricante llevó a cabo una campaña publicitaria sobre su seguridad. Los defensores de la Fuerza Aérea propusieron crear un sistema de niveles múltiples añadiendo terminales remotas desprotegidas, para usos sin clasificar, a fin de lograr mayor coordinación y eficiencia. Nuevamente, las contraseñas iban a proteger la información sensible. Cuando un usuario presentó su contraseña a la computadora, GCOS comprobó una lista de contraseñas para verificar la legitimidad del usuario. Para hacer esta comprobación, GCOS copió parte de la lista en su memoria principal. Entre otros defectos, el equipo de expertos técnicos averiguó que GCOS dejó esta copia de las contraseñas donde pudieran imprimirse fácilmente y sin trazas. Los diseñadores habían pasado por alto la posibilidad de un uso indebido deliberado de una función de computadora necesaria.

*Los diseñadores del gobierno no son perfectos.* Después de la penetración en el Pentágono, algunos defensores afirmaban que los diseñadores del gobierno con un mayor conocimiento de seguridad podrían evitar dichos defectos. Una organización que procesaba datos de inteligencia sensible hicieron uso de un esfuerzo sustancial “arreglando” básicamente el mismo sistema GCOS. Tenían confianza de que podrían mantener la seguridad de modalidad de niveles múltiples. El equipo de expertos técnicos averiguó que estos “arreglos” podrían evitarse fácilmente. En este caso no solo podría cualquier usuario obtener cualquier información en el sistema sino que también podría tener acceso a información clasificada en computadoras conectadas en una red con esa computadora.

*Un contrato no puede dar seguridad.* Básicamente se seleccionó el mismo sistema GCOS para un sistema de mando y control importante. Los defensores aseguraron a los usuarios que estaría protegido en múltiples niveles porque la seguridad era requerida por el contrato. Una amplia evaluación del equipo de expertos técnicos dio a conocer que había muchos defectos de seguridad profundos y complejos que desafiaban la reparación práctica—se opinó que la computadora no solo finalmente no protegía sino que no se podía proteger.

*La mejor seguridad no es suficientemente buena.* Honeywell Information Systems, con patrocinio del DOD, modificó la computadora GCOS en un esfuerzo para mejorar sustancialmente varias áreas, incluida la seguridad. El resultante servicio Multiplexed Information and Computing Service (Multics) fue muy alabado por su seguridad. El equipo de expertos técnicos usó una computadora de laboratorio de la Fuerza Aérea para evaluar Multics como computadora de protección potencial de múltiples niveles para el Pentágono. Aunque tenía el mejor diseño de seguridad de todos los sistemas encontrados, el equipo de expertos técnicos halló varios defectos de implementación.<sup>12</sup> En un caso, Multics comprobó primero una posible autorización del usuario para acceder a la información y, cuando la solicitud demostró ser válida, ejecutó la solicitud. No obstante, el usuario pudo cambiar la solicitud después de la comprobación de validez pero antes de la ejecución; Multics ejecutó después la solicitud cambiada, permitiendo un acceso sin autorización. Esta penetración de Multics provino de un atajo de implementación para mejorar la eficiencia.

*Contraseñas codificadas recuperadas.* El sistema Multics codificó internamente su lista de contraseñas de modo que incluso impresas, las contraseñas no eran ininteligibles. Cuando un usuario presentó su contraseña, se codificó y después se comparó con la lista codificada. El equipo de expertos técnicos usó el método de penetración desarrollado en la computadora del laboratorio

para acceder a la lista de contraseñas codificadas de una universidad grande y después descifró el código para obtener todas las contraseñas.

*Trampilla instalada.* El equipo de expertos técnicos penetró en Multics y modificó la copia maestra del fabricante del sistema de operación Multics mismo instalando una trampa: las instrucciones de la computadora para omitir deliberadamente los controles de seguridad normales y asegurar así la penetración incluso después de haber arreglado el defecto inicial. Esta trampa era pequeña (menos de 10 instrucciones de 100.000) y requería una contraseña para usarla. El fabricante no pudo encontrarla, incluso cuando sabía que existía y cómo funcionaba. Además, desde que se insertó la trampa en la copia maestra de los programas del sistema de operación, el fabricante distribuyó automáticamente esta trampa a todas las instalaciones Multics.

*Registro de auditoría destruido.* Algunos han discutido que una necesidad de computadora no impide siempre un acceso no autorizado siempre que se mantenga un registro de auditoría de dichos accesos. El sistema Multics mantenía un registro de auditoría protegido de acceso, y se registraron los accesos sin autorizar del equipo de expertos técnicos. No obstante, el registro de auditoría estaba por sí mismo sujeto a un acceso sin autorizar. El equipo de expertos técnicos modificó meramente el registro para borrar todas las trazas de sus acciones, como la inserción de la trampa.

*Incluso los arreglos tienen defectos.* Honeywell produjo una nueva computadora Multics que corrigió todos los defectos de implementación informados por el equipo de expertos técnicos. Este equipo usó la computadora nueva de Honeywell en su fábrica de Phoenix, Arizona, y penetró nuevamente en el sistema de seguridad.<sup>13</sup> ¡Este nuevo defecto fue debido a cambios hechos para corregir los cambios anteriores! Se iba haciendo cada vez más claro que proporcionar una computadora segura a múltiples niveles era realmente difícil.

*El caballo troyano no está muerto.* Aunque algunos habían reconocido el problema, los defensores que pertenecían al Estado Mayor Aéreo alababan una instalación por su solución de seguridad de niveles múltiples en otra computadora. La solución consistía en programas para segregar la información en clasificada y sin clasificar. No había terminales remotas, pero los usuarios podían enviar trabajos sin clasificar a la computadora sin controles de seguridad. A partir de un trabajo sin clasificar, el equipo de expertos técnicos penetró en el sistema fundamental de computadoras y modificó la solución en un caballo troyano, un programa aparentemente útil que ocultaba capacidades perjudiciales. El caballo troyano ocultó una copia invisible de trabajos clasificados. Un trabajo posterior sin clasificar recuperó la información oculta, poniendo en riesgo la seguridad. Así pues, la solución de seguridad no solamente era ineficaz sino que realmente acentuaba el problema de seguridad.

*La moraleja evidente.* Pocos o ningún control de seguridad de computadora contemporáneo han impedido a un equipo de expertos técnicos un acceso fácil a cualquier información buscada. Estos ejemplos no son completos de ninguna manera; no deben usarse para inferir la predominancia de ciertos defectos o asociar debilidades particulares con tan solo unos pocos fabricantes. Otros tienen problemas de seguridad comparables.

### ***Futilidad de evaluación por penetración***

La Fuerza Aérea, en un sentido muy real, ha sido afortunada de que la seguridad sea tan deficiente en las computadoras actuales—el mayor peligro vendrá cuando parezca plausible el argumento de que una computadora es segura porque los equipos de expertos técnicos no pudieron penetrar en ella. De hecho, la evaluación de controles de seguridad de computadoras internas es un reto muy difícil. Como en el caso de la criptografía, hay básicamente dos métodos.

Si los controles de seguridad se basan en una tecnología firme cuidadosamente formulada, entonces pueden estar sujetos a un análisis racional de su eficacia. Como ya se ha observado, esto

no es generalmente cierto en las computadoras contemporáneas. También se tratará el método del núcleo de seguridad, que está sometido a un análisis técnico tan metódico.

De forma alternativa, un defensor puede simplemente buscar formas de penetrar en los controles de una computadora; al no poder penetrar, puede discutir plausiblemente que no hay forma de penetrar, ya que no conoce ningún método. Si se encuentra una falla de seguridad, primero puede parchearse antes de discutir de la seguridad. Evidentemente, este argumento tiene muchas dificultades teóricas y prácticas.

En principio, uno podría probar todos los programas posibles para encontrar uno que permita una penetración en el sistema de seguridad. Este método de agotamiento sería efectivo pero está muy lejos de ser viable. ¡Para cualquier computadora sustancial esto llevaría tanto tiempo que antes de acabar la evaluación el sol se habría consumido! Así pues, una evaluación realizable por agotamiento debe ser tan incompleta como ridícula.

De hecho, el esfuerzo hecho en penetrar y parchear produce un retorno marginal deficiente en términos de seguridad. Los ejemplos de equipos de expertos técnicos indican algunas de las dificultades:

En primer lugar, la experiencia muestra que los nuevos perpetradores tienden a encontrar nuevos defectos—incluso después de que equipos anteriores hayan encontrado todo lo que pudieron. Parece poco probable que un atacante real no involucre a nuevas personas.

En segundo lugar, los defectos no son producto generalmente de una estupidez general sino que se deben a descuidos humanos al tratar un problema de diseño difícil. Así pues, los arreglos mismos probablemente tengan defectos.

En tercer lugar, no se requiere un experto muy especializado para penetrar en el sistema de seguridad. Es cierto que la mayoría de los profesionales informáticos no conocen formas de penetrar en los sistemas que usan; desean hacer un trabajo, no interferir con él. No obstante, cuando se les da la asignación, incluso los profesionales menos experimentados e inexperimentados han tenido éxito uniformemente en penetrar en el sistema de seguridad.

En cuarto lugar, la exposición al ataque es frecuentemente mucho mayor que simplemente la procedente de usuarios conocidos del sistema. Las conexiones telefónicas comerciales con sistemas militares están aumentando y permiten el acceso desde todo el mundo. Las intercepciones de comunicaciones también permiten el acceso a conexiones directas sin asegurar; las intercepciones de microondas por parte de los soviéticos en EE.UU., como reveló recientemente la Casa Blanca, demuestran esta capacidad. La falta de control de seguridad estricta en el envío de trabajos de computadora permite ataques en nombre de un usuario legítimo incluso para computadoras sin terminales remotas. La interconexión con otras computadoras puede añadir también un grupo grande de usuarios desconocidos.

En quinto lugar, los ataques pueden desarrollarse y perfeccionarse en otras computadoras menos en la computadora objetivo. Una computadora similar propiedad o accedida legítimamente por el atacante pueden usarse para minimizar el riesgo de detección. Una vez perfeccionado, los métodos de ataque pueden aplicarse a la computadora objetivo.

Por último, para un penetrador hostil, los métodos de trampa y caballo troyano son probablemente los más atractivos, y estos defectos creados deliberadamente en programas informáticos son las más difíciles de detectar. La mayoría de los equipos de expertos técnicos se concentran en defectos accidentales que nadie podría encontrar, pero los defectos deliberados están latentes hasta que son activados por un atacante. Estos errores pueden colocarse prácticamente en cualquier lugar y diseñar cuidadosamente para escapar la detección. No obstante, la mayoría de los sistemas militares incluye programas no desarrollados en un entorno seguro, y algunos incluso se desarrollan en el extranjero. De hecho, algunos sistemas pueden ser subvertidos por un técnico remoto anónimo sin una función legítima en el desarrollo del sistema. Estos errores pueden activar esencialmente cualquier interfaz externa—desde un telegrama sin clasificar a una situación única establecida para la detección por un sistema de vigilancia.

En resumen, la penetración y el parche de controles internos no es una técnica de seguridad prometedora. Incluso sin la posibilidad de trampillas y caballos troyanos y sin demandas de seguridad militares, “las compañías privadas han tratado siempre de parchear defectos en los llamados sistemas de computadoras [seguros], y después de millones de dólares y años de esfuerzo, cedieron antes el fracaso”.<sup>14</sup> Este método es poco más que un juego de inteligencia en el que el diseñador debe tratar de encontrar (y parchear) *todos* los defectos mientras el enemigo necesita encontrar (y explotar) todo menos un defecto restante—una contienda bastante desequilibrada.

El “resultado final” es simple. El comandante responsable de la seguridad en un sistema informático necesita una respuesta inequívoca a una pregunta crucial: ¿depende la seguridad de los controles internos? Es decir, ¿hay alguna falla o subversión de la computadora misma que podría degradar la seguridad? Si es así, con las computadoras contemporáneas tiene una falta de uniformidad radical en la laxitud sobre la seguridad de computadoras dentro del entorno militar que normalmente tiene controles estrictos sobre la diseminación de información sensible.

## Alternativas de seguridad de computadoras

Hemos visto que en las computadoras contemporáneas los controles internos no solo son ineficaces sino que también desafían la evaluación. No obstante, evidentemente podemos seguir la ruta de la experiencia criptográfica alemana y japonesa—subestimar la explotación enemiga de la debilidad técnica. Esta es el riesgo que hemos corrido en cada una de las diversas decisiones de la Fuerza Aérea para operar computadoras contemporáneas en una modalidad de múltiples niveles.

Si perdemos esta apuesta, el daño depende de qué está protegiendo la computadora. Puede variar desde la violación de la privacidad personal hasta el fraude, daños en el campo de batalla o ataque sorpresa preventivo. Por ejemplo, se ha propuesto que la Fuerza Aérea cambie dinámicamente los objetivos de sus misiles balísticos estratégicos; esto apoya la política nacional de respuesta flexible y permitiría la aplicación de armas de represalia para los objetivos militares lucrativos. Sin embargo, las computadoras están en el centro de esta capacidad; si fueran penetradas, un enemigo podría cambiar los objetivos de los misiles para que impacten en objetivos de poco valor o incluso en objetivos amigos como parte de un ataque por sorpresa.

No trataremos de explorar las numerosas posibles situaciones de dependencia de las técnicas débiles, pero nos fijaremos en soluciones alternativas. Comprenden asuntos técnicos y de política. Básicamente, la Fuerza Aérea tiene dos alternativas además de hacer caso omiso del problema: limitar el uso de computadoras o usar la tecnología adecuada disponible para hacer que los controles internos sean más fiables.

### *Evite la dependencia de los controles internos*

La alternativa evidente es restringir de forma deliberada el uso de computadoras a una modalidad especial de modo que los controles internos no puedan afectar la seguridad. Hay tres formas comunes de evitar la dependencia en los controles internos.

En primer lugar, se puede dedicar una computadora separada a cada nivel de información clasificada. Esto es particularmente atractivo para un sistema en línea o de tiempo real donde la información debe ser inmediatamente accesible. Este método puede conducir a computadoras duplicadas o usadas de modo ineficaz.

En segundo lugar, cada nivel de información clasificada puede programarse para usar la computadora para un período diferente. Esto requiere purgar información de toda la memoria del sistema al final de un período programado. Este procedimiento manual normalmente engorroso carece de capacidad de respuesta y desperdicia los recursos informáticos mientras se completa el nivel de clasificación.

En tercer lugar, se pueden procesar varios niveles de clasificación juntos. Todas las líneas de comunicación deben protegerse, y todos los usuarios necesitarían ser un acceso autorizado a toda la información. Como los controles internos no son fiables, todo el producto del sistema está clasificado temporalmente como del máximo nivel. Para obtener información con una menor clasificación, una autoridad competente debe revisar manualmente la salida de contaminación y rebajarla antes de descargarla en el nivel inferior.

Estas restricciones de uso son compatibles con una buena seguridad, pero resultan en una degradación sustancial de capacidad en una computadora moderna.

*Gastos adicionales.* Estas restricciones de seguridad aumentan considerablemente el costo. Se necesitan medidas de seguridad de comunicación adicionales, y mano de obra adicional para la revisión manual de la salida. Existe también el costo de las investigaciones de aprobación de seguridad para los usuarios cuya información la computadora podría contaminar con información de una clasificación más elevada. Otros costos incluyen aquellos para equipos duplicados y la capacidad adicional para compensar los recursos desperdiciados. Por ejemplo, cuando un sistema de computadoras importante no provea la seguridad prometida de niveles múltiples, los sitios principales de la Fuerza Aérea tenían que aprobar a muchos usuarios y hacer compras de múltiples millones de dólares de equipos adicionales.

*Mayor riesgo.* En la práctica la modalidad especial conduce a un aumento importante en la exposición de información. La falta de controles internos destruye efectivamente la división en compartimientos prevista para limitar el daño de la subversión. El mayor número de personas que requieren aprobación aumenta la probabilidad de dar acceso a un individuo en el que no se puede confiar. Los procedimientos de purga manuales tienen tendencia a errores que dejan residuos de memoria clasificada que pueden ser extraídos por usuarios no autorizados. Además, la revisión manual de grandes volúmenes de salida de computadora puede ser de hecho una argucia burocrática para transferir responsabilidad de seguridad de los diseñadores a los usuarios; el revisor tiene poca probabilidad de detectar información clasificada sin autorizar que haya estado incluida de forma accidental o incluida de forma deliberada en la salida.

*Capacidades inevitables.* Dichas restricciones de seguridad pueden limitar seriamente la capacidad de operación de los sistemas de apoyo en el campo de batalla. Las armas modernas exigen sistemas de mando y control con un acceso rápido a una base grande de información actual y exacta. Esta base de datos (necesariamente compartida e integrada) contendrá típicamente información que va de sin clasificar a muy secreta. Como muchas personas que mantienen la información menos clasificada tienen autorizaciones limitadas, y el volumen de información requiere el uso de computadoras, tenemos el problema de seguridad clásico de múltiples niveles. Los controles internos de la computadora son cruciales para proteger la información, y evitar la dependencia en los controles internos limitará seriamente las capacidades del sistema.

El problema se acentúa por la interoperabilidad con su red interconectada de computadoras con una comunidad de usuarios grande, diversa y geográficamente dispersa. Las redes de computadoras de sistemas de mando y control son un ejemplo importante. No obstante, un oficial militar observó que debido a la seguridad deficiente de las computadoras internas en una de dichas redes, sus computadoras 35 de gran escala de uso general nunca se usarían verdaderamente para la finalidad para la que se compraron. El problema se agrava aún más por la mayor necesidad de fusión de información de inteligencia seleccionada (sin arriesgar fuentes sensibles) con información de operaciones tácticas.

En resumen, la modalidad especial evita muchos problemas de seguridad de la computadora pero no satisface las necesidades de operación de una fuerza militar moderna. Estas necesidades solo se pueden satisfacer mediante la protección eficaz de múltiples niveles en la computadora misma.

*Aplique una tecnología adecuada*

El desarrollo y la aplicación de seguridad de computadoras internas fiables no son sencillos ni imposibles. Aunque frecuentemente se reconoce la necesidad de una operación de múltiples niveles, las fuerzas armadas han prestado solamente atención al desarrollo de la tecnología requerida. De hecho, la Fuerza Aérea dirigió recientemente la terminación de su programa de desarrollo de seguridad de múltiples niveles, el mayor en el Departamento de Defensa.<sup>15</sup>

Antes de que examinemos el avance tecnológico que se ha hecho, debe resultar instructivo identificar parte del razonamiento que afloró en la terminación reciente de la Fuerza Aérea. La pauta de ideas refleja que la seguridad de computadoras no es actualmente un foco importante.

- La posibilidad de que la industria resuelva el problema de seguridad de las computadoras se ha sobrestimado al llegar a la conclusión de que la industria tiene el mismo problema de seguridad que las fuerzas armadas. No obstante, la analogía de comunicaciones indica una dificultad. En el sector civil, las violaciones de seguridad de comunicaciones están sometidas a legislación, no a prevención; los micrófonos ocultos son ilegales, y hay un resarcimiento legal para la pérdida. Por el contrario, las fuerzas armadas deben acudir a la prevención (por ejemplo, criptografía aprobada por los militares), ya que no podemos llevar a juicio a la KGB. La situación de las computadoras es similar; hay impulsos legislativos pero un éxito comercial limitado para lograr controles internos demostrablemente efectivos. La espera de soluciones espontáneas para la industria es probable que sea larga, y es poco probable que cumplan con las normas de seguridad militar en áreas como la protección contra la subversión deliberada.
- La financiación inadecuada de la investigación y del desarrollo (I+D) se asignó para continuar un elemento del programa a un nivel óptimo. No obstante, hay partes del programa con fondos disponibles que también se terminaron. Se completaron con éxito ocho millones de dólares de EE.UU. de trabajo. Quedaron unos 10 millones de dólares de EE.UU. de trabajo en más de cuatro años para completar el desarrollo de un prototipo completo y la base general asociada para efectuar compras competitivas. Varias estimaciones indican que los costos de desarrollo pueden recuperarse evitando las sanciones de la modalidad especial—sin mencionar la mayor capacidad de seguridad y operación.
- La amenaza se minimiza buscando contrainteligencia que no está prácticamente disponible, por ejemplo, ejemplos reales de agentes enemigos sorprendidos en el acto. El enemigo puede parecer demasiado ignorante para la penetración, no interesado en secretos militares, o incapaz de una subversión y explotación planificadas. Una cuantificación de un solo número de la probabilidad de amenaza puede suponer implícitamente un incidente aleatorio en vez de una actividad de penetración planificada. Esto puede indicar un riesgo sin un criterio objetivo de aceptabilidad. Estas percepciones no se basan generalmente en métodos de inteligencia profesional con “ejemplos trabajados” (por ejemplo, de seguridad de comunicaciones) de la metodología.
- El interés en desarrollar soluciones está limitado por una falta clara de responsabilidad de la eficacia de controles internos. Las oficinas de estado mayor y política pueden dar recomendaciones, guiar e incluso aprobar mecanismos de seguridad informáticos sin responsabilidad por cualquier riesgo de seguridad que pueda resultar. Por otra parte, la prueba de seguridad y los esfuerzos de evaluación y las asesorías económicas de comandantes individuales están en gran medida sin relacionar con la protección real del sistema. Esto es claramente contrario a la seguridad de comunicación militar donde los expertos técnicos son responsables de certificar los mecanismos de seguridad.

- El problema de seguridad informática es difícil de reconocer cuando la política no distingue claramente los casos donde la computadora simplemente proporcione cálculo y donde la computadora proporcione protección interna. Dicha política se concentra en el desarrollo de controles de seguridad que “no son necesariamente certificablemente perfectos”—un objetivo bastante ambiguo. En dicha estructura de política, los análisis no identificarán la necesidad de controles internos. De hecho, una computadora podría satisfacer bien todos los reglamentos y seguir siendo muy vulnerable.
- La confianza en controles débiles aumenta debido a la suposición de que el gasto en recursos de seguridad la mejorará sustancialmente. De hecho, el esfuerzo puede ser simplemente ineficaz, como en el caso del interminable penetrar y parchear. La política actual enumera características de diseño de computadoras para la seguridad interna que no son ni necesarias ni suficientes para la seguridad.
- La atención a los trucos de seguridad hace que no nos fijemos en debilidades importantes. Hay muchos mecanismos de eficacia mínima para mejorar los controles de seguridad interna—analizadores de escritura a mano, codificación de datos internos, memoria de solo lectura para información de seguridad, etc. Cierta guía ha animado a los programas de computadora que clasifican y etiquetan productos por nivel de seguridad. La evaluación de estos programas se concentra en resultados esperados con usuarios amigos en vez de la subversión deliberada de los programas o la penetración del sistema fundamental. Llevar a cabo dichos esfuerzos aislados frecuentemente es peor que no hacer nada, ya que da un falso sentido de seguridad.

Estas clases de problemas hicieron que la Fuerza Aérea considerara su programa de desarrollo de la División de Sistemas Electrónicos (recientemente terminado) como “controvertido”. Pero nuestro examen previo del problema hace claro que la operación a múltiples niveles sin una tecnología adecuada es una apuesta de alto riesgo. Como mucho, es extrañamente poco coherente con las normas establecidas en otras áreas (por ejemplo, comunicaciones) de seguridad militar que hacen una hipótesis de una amenaza hostil deliberada, competente y motivada y responde con contramedidas efectivas. Lo más probable es que anule las demás medidas de seguridad, permitiendo un daño limitado solo por la imaginación del enemigo.

## Tecnología del núcleo de seguridad

Afortunadamente, la I+D militares—en particular el programa de la Fuerza Aérea recientemente terminado,<sup>16</sup>—ha logrado un avance sustancial hacia la tecnología adecuada para lograr una seguridad de múltiples niveles. Un paso importante hacia la solución fue la introducción en 1972 de la tecnología del núcleo de seguridad<sup>17</sup>, que proporcionó una base científica demostrablemente eficaz de los controles de seguridad internos. Aunque una explicación de los detalles técnicos va más allá del alcance de este artículo, un informe técnico resume el método del núcleo de esta forma:

El método para obtener un sistema seguro comprende primero definir los requisitos de seguridad y después crear un diseño conceptual que pueda mostrarse para proporcionar la protección requerida (es decir, un modelo). El modelo define formalmente un sistema ideal (en nuestro caso uno que cumpla con los requisitos de seguridad militar), y proporciona una base para probar una implementación subsiguiente. Una vez que se haya implementado [un núcleo de seguridad] que cumpla con los requisitos descritos anteriormente, se habrá logrado la seguridad de las computadoras. Del software en el sistema, solamente el núcleo de seguridad . . . necesita corregirse . . . El sistema operativo propio o el software de aplicación pueden contener desperfectos introducidos de forma inadvertida o trampillas maliciosamente plantadas sin arriesgar la seguridad.<sup>18</sup>

Según el programa de la Fuerza Aérea el núcleo demostró su viabilidad técnica, independientemente de cualquier vendedor de computadoras particular o política de seguridad. El núcleo también ha establecido considerablemente su aceptabilidad operacional, con evidencia específica para una amplia funcionalidad, buena eficiencia, capacidad de certificación de seguridad y compatibilidad. Además, los requisitos técnicos básicos del núcleo se han incorporado con éxito a las especificaciones de compras militares para una computadora comercial a gran escala y una computadora de sistemas de armas empotrada. En pocas palabras, la tecnología básica está muy a mano.

### *Fundamento científico*

Un núcleo de seguridad es un pequeño conjunto de instrucciones de programas de computadora y equipos asociados que controla todo el acceso por parte de los usuarios (es decir, a través de sus programas) a la información. Un núcleo de seguridad dado es normalmente exclusivo de una computadora particular. Un núcleo de seguridad para computadoras es de muchas maneras conceptualmente análogo a un dispositivo criptográfico para las comunicaciones.

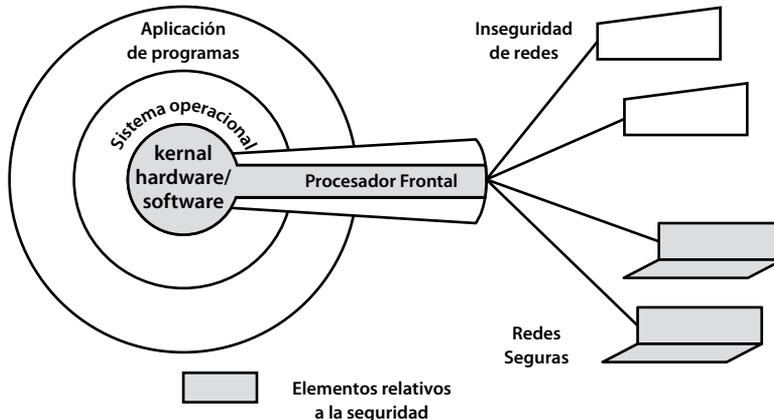
El diseño del núcleo de seguridad se deriva directamente de esa especificación precisa (es decir, un modelo matemático) de su función. (El modelo de núcleo es análogo al algoritmo que define la función matemática de un dispositivo criptográfico). Este modelo matemático es una formulación precisa de reglas de acceso basadas en atributos del usuario (autorización, necesidad de saber) y atributos de información (clasificación). Los parámetros del sistema controlan el uso específico de una instalación (por ejemplo, para la política de clasificación del DOD, protección de privacidad, etc.).

La característica de distinción fundamental (de ahí su nombre) del concepto de núcleo de seguridad es que un núcleo representa un perímetro de seguridad interno distinto. En particular, esa porción del sistema responsable de mantener la seguridad interna se reduce desde esencialmente toda la computadora hasta principalmente el núcleo. Así pues el núcleo es análogo a un dispositivo criptográfico que elimina la mayor parte de una ruta de comunicación de la consideración de seguridad. Para ser un poco más técnico y concreto, un núcleo de seguridad típico tiene varios (digamos que de diez a veinte) programas de computadora pequeños (es decir, subrutinas) que pueden ser invocadas por otros programas (por ejemplo, el sistema operativo y los programas de aplicaciones de usuario individuales). El núcleo, y solo el núcleo, controla y gestiona todos los componentes de hardware que almacenan y acceden a información. Los demás programas (es decir, no nucleares) deben invocar el núcleo (es decir, llamar a sus subrutinas) para tener acceso a la información—el núcleo comprueba el usuario y los atributos de información y permite solo acceso que esté autorizado. Sin embargo, a pesar de estas comprobaciones, existe un impacto mínimo del usuario. La Figura 1 ilustra conceptualmente esta estructura.

El avance técnico significativo fue el descubrimiento de un conjunto de funciones de modelos y condiciones que son probablemente suficientes para impedir riesgos a todos los posibles programas de computadora que no sean de núcleo. Cada función del modelo determina el diseño de un programa de núcleo. Además, el modelo impone condiciones de seguridad que el diseño debe cumplir. Se han demostrado teoremas de seguridad que muestran que el núcleo (al seguir precisamente el modelo) no permitirá un riesgo, sea cual sea el programa que lo use o cómo lo use. Es decir, el diseño del núcleo es a prueba de penetraciones—en particular a todos esos ataques inteligentes que nunca tuvieron en consideración los diseñadores de núcleos.

Esta base de plenitud matemática sube el nivel del diseño del núcleo y del proceso de evaluación por encima de un mero juego de ingenio con un atacante; esto es análogo a la teoría de información como base de un criptoanálisis moderno. Un efecto dramático es que el núcleo facilita la evaluación objetiva de seguridad interna. El evaluador no necesita examinar el casi ilimitado número de posibles intentos de penetración; solamente necesita verificar que el modelo

matemático esté correctamente implementado por el núcleo. En otras palabras, el núcleo proporciona los controles internos verificablemente fiables necesarios para la seguridad de múltiples niveles.



**Figura 1. Sistema de computadora seguro**

### *Viabilidad de ingeniería*

Para ser útil, el concepto de núcleo no debe ser solamente matemáticamente firme sino también viable de implementar. La implementación satisfactoria se basa en tres principios de ingeniería:

*Plenitud.* Se debe invocar un núcleo de seguridad cada vez que se acceda a datos en la computadora.

*Aislamiento.* Se debe proteger un núcleo de seguridad y su base de datos contra la modificación no autorizada.

*Capacidad de verificación.* Un núcleo de seguridad debe ser suficientemente pequeño y simple de modo que su función pueda probarse y verificarse completamente.

Un núcleo de seguridad de laboratorio para una minicomputadora comercial (Digital Equipment Corporation modelo PDP-11/45) mostró tener viabilidad en 1974. El hardware de “memoria virtual” de esta computadora era una ayuda significativa para asegurar la plenitud y el aislamiento del núcleo. Este núcleo en funcionamiento constaba solo de unas 1000 instrucciones de computadora. El experimento también estableció que es mucho más fácil introducir el concepto de núcleo en un diseño inicial que modificarlo más adelante.

La base del diseño (es decir, modelo de núcleo) se verificó matemáticamente. Como con los dispositivos criptográficos, la verificación de la implementación correspondiente se basaba más en un diseño de ingeniería cuidadoso y pruebas extensas que en matemáticas formales. Las pruebas automáticas y las técnicas de verificación de programas indicaban que la implementación del núcleo correspondía al diseño. Este prototipo de laboratorio confirmó la viabilidad pero no estaba orientado hacia la evaluación de rendimiento y eficiencia. De pasada, es interesante observar que un equipo de expertos técnicos trató de penetrar su seguridad pero no pudo.

### *Rendimiento*

Se examinó el rendimiento en un sistema de computadoras más grande. Se experimentó una degradación muy pequeña del rendimiento (menos de un 1 por ciento) cuando se modificó el Multics comercial (para la gama 6000 de Honeywell) al modelo de núcleo. Esta versión de Multics no se implementó como un verdadero núcleo, es decir, los controles se distribuyeron en vez

de recopilarse en una entidad pequeña verificable; no obstante, esta versión hizo todos los controles de seguridad requeridos en un núcleo y así confirmó que el núcleo no era inherentemente ineficiente.

Las buenas características de seguridad del hardware del núcleo fueron un auxiliar importante para el rendimiento, y estas características eran independientes del vendedor. La versión tuvo tanto éxito que Honeywell incluyó el Mecanismo de Aislamiento de Acceso resultante en ofertas comerciales Multics para la protección de la privacidad y la información comercial. Este sistema se usó como base del prototipo de Fuerza Aérea terminado; el desarrollo prototipo fue implementar un núcleo verdadero verificable.

### ***Funcionalidad***

Un núcleo de seguridad fuerza al usuario de la computadora a pensar en la seguridad pero no degrada gravemente las capacidades de la computadora. Esto se demostró claramente cuando se instalaron con éxito las modificaciones de Multics para esos usuarios exigentes en el Pentágono: las limitaciones del diseño del núcleo tenían un impacto adverso mínimo en los usuarios. Así como la criptografía permite el uso seguro de equipos de comunicación comerciales, el concepto de núcleo permite el uso seguro de equipos y programas de computadora comerciales estándar. La instalación del Pentágono con su procesamiento clasificado confirmó los conceptos de apoyar una computadora basada en núcleo en un contexto de seguridad total del sistema.

La utilidad operacional del núcleo se demostró adicionalmente con el prototipo de minicomputadora inicial. Una demostración mostró la interfaz de operaciones segura y sistemas de inteligencia para la fusión de la información táctica del campo de batalla. Además, varios esfuerzos militares de I+D en varias etapas de terminación han usado elementos importantes de la tecnología del núcleo de seguridad: una red de mando y control, un controlador criptográfico, un sistema de comunicación digital nacional, un sistema “monitor de máquinas virtual” a gran escala, un sistema operativo de minicomputadora general y una minicomputadora militarizada segura (basada en el Nivel 7 Honeywell comercial). Aunque confirman la utilidad del núcleo de seguridad, ninguno de esos esfuerzos de I+D conducirá a disponibilidad y uso operacional generales.

### ***Política de seguridad***

Aunque el concepto de núcleo de seguridad no contradice la política actual, la política futura debe reconocer y aprovechar las características del núcleo. La política debe reconocer que el modelo matemático proporciona una forma de traducir las reglas de seguridad tipo papel y lápiz en términos informáticos. Además, una política significativa para la modalidad de múltiples niveles reflejaría las realidades tecnológicas: o todo el sistema debe ser correcto (no viable actualmente) o se debe usar el núcleo de seguridad.

En lo que respecta a dispositivos criptográficos, el núcleo debe protegerse contra la subversión (por ejemplo, inserción de una trampa) durante su desarrollo. Pero proteger el núcleo ciertamente involucra a muchas menos personas y a un entorno más controlado que tratar de proteger todos los programas de computadora del sistema; así pues, en contraste con los sistemas contemporáneos, el núcleo hace que sea tratable proteger contra la subversión. Además, la evaluación (para la certificación) de controles internos de seguridad de computadoras es una tarea técnica difícil. El método del núcleo para el diseño y la implementación hace viable dicha certificación, pero esta evaluación sigue requiriendo expertos técnicos muy capaces—así como la evaluación de dispositivos criptográficos.

Este método conceptualmente se asemeja a la criptografía militar moderna. (Vea la Tabla II). Sin embargo, se debe reanudar el desarrollo y se deben hacer ajustes de política si se va a poner a disposición en general en cualquier momento en un futuro inmediato. Para estar seguros, hay demandas que compiten en recursos. El desarrollo de armas empleables directamente (como

aviones caza) puede tener siempre una mayor prioridad que el desarrollo de seguridad de computadoras, pero según lo explicó un observador: “¿Cómo serían de efectivos esos aviones caza si los planes para su empleo fueran conocidos por adelantado por un adversario que hubiera penetrado en la computadora que contenía esos planes?”<sup>19</sup> El núcleo de seguridad es claramente la única tecnología disponible en la actualidad que puede proporcionar las capacidades de seguridad y operacionales que debemos tener.

**Tabla II. Puntos comunes en tecnología de seguridad**

	<b>Mecanismo criptográfico</b>	<b>Núcleo de seguridad</b>
amenazas negadas..... en vez de ilegalizadas	micrófonos ocultos	penetración
elementos comerciales..... estándar preservados	circuitos de comunicación	computadoras y programas
porciones limitadas ..... sensibles a la seguridad	principalmente el cripto	principalmente el núcleo
base fundamental ..... formulada de forma precisa	algoritmo criptográfico	modelo matemático
evaluación de diseño..... criterios definidos	teoría de información	teoremas de seguridad
implementación que cumple..... exactamente el diseño	ingeniería metódica	programas verificados
subversión controlada..... por seguridad física	fabricación	programación
expertos diestros necesarios..... para la certificación	criptoanalistas e ingenieros	científicos informáticos

La seguridad a menudo requiere opiniones subjetivas, y algunas personas pueden diferir con el autor sobre puntos específicos. En general, parece evidente que un usuario que confíe ciegamente en la protección proporcionada por computadoras para obtener información militar sensible pondrá en peligro seriamente la seguridad. De hecho, la mayoría de las computadoras no incluyen ni siquiera las características nominales para apoyar un sistema de seguridad militar. Incluso cuando lo hacen, la esencia del problema de seguridad de la computadora es la eficacia técnica de los controles internos, y la evidencia es clara de que la mayoría de los controles internos no son fiables.

Por otra parte, la limitación del uso de computadoras para evitar este problema es costosa y nos priva de la capacidad operacional vital. El dilema de eficacia en comparación con la eficiencia genera presión para subestimar la amenaza y el exceso de confianza de controles de seguridad internos. Desgraciadamente, estas presiones han conducido a la Fuerza Aérea a una dependencia perturbadora y en aumento sobre los controles de seguridad débiles incluso en ausencia de evidencia de eficacia.

La Fuerza Aérea terminó recientemente el único programa de DOD importante para proporcionar controles internos científicamente firmes—controles basados en el concepto de núcleo de seguridad. El desarrollo del pasado ha demostrado claramente la viabilidad, el rendimiento y la utilidad de esta tecnología. No obstante, debido a la carencia de un entendimiento técnico y

una política significativa, existe en la actualidad poco apoyo oficial para el desarrollo de esta capacidad prometedora.

Se deben tomar tres medidas básicas para controlar el impacto del adversario de nuestra debilidad de seguridad de computadora:

- Promulgar una política clara que distinga entre dependencia en controles externos (modalidad especial) y controles internos (modalidad de múltiples niveles). No debe ser posible satisfacer la política sin proporcionar una seguridad de forma genuina. La modalidad de múltiples niveles sin una base técnicamente firme debe estar expresamente prohibida.
- Incorporar controles de seguridad militarmente explícitos en sistemas de procesamiento clasificados. Deben estar basados en una especificación precisa de las funciones requeridas (como en el modelo de núcleo para Multics del Pentágono). Este paso es crucial para la futura introducción de seguridad de múltiples niveles sin un rediseño de sistema completo. (Entretanto, esto puede ayudar a proteger la privacidad y los recursos valiosos).
- Reanudar el desarrollo del núcleo de seguridad para proporcionar seguridad de múltiples niveles técnicamente firme. Como en el programa anterior de la Fuerza Aérea, esto debe orientarse hacia el proceso de adquisición militar competitivo. Al mismo tiempo, la política debe cambiarse para facilitar el uso operacional de la tecnología de núcleo.

No es fácil hacer que un sistema de computadoras sea seguro, pero tampoco es imposible. El mayor error es no hacer caso al problema—un error fatal que evidentemente permite que sigan sin usarse soluciones disponibles. El error en esta área crítica introduce un talón de Aquiles en nuestros sistemas de apoyo del campo de batalla—la piedra angular de la Fuerza Aérea electrónica moderna.

*Escuela Naval de Posgraduados  
Monterey, California*

#### Notas

1. Malcolm R. Currie, "Electronics: Key Military 'Force Multiplier' " (Sistemas electrónicos: multiplicador de las fuerzas militares clave), *Air Force Magazine*, julio de 1976, p. 44.

2. Edgar Ulsamer, "How ESD Is Building USAF's Electronic Eyes and Ears" (Cómo el ESD está formando los ojos y oídos electrónicos de la USAF), *Air Force Magazine*, julio de 1977, p. 40.

3. La importancia de la electrónica de la Fuerza Aérea se indica en "The Electronic Air Force" (La fuerza aérea electrónica), *Air Force Magazine*, julio de 1977, p. 29, que observa que este es el séptimo ejemplar anual de la revista dedicado principalmente a este "problema fundamental de la Fuerza Aérea".

4. F. W. Winterbotham, *The Ultra Secret (El secreto Ultra)* (New York: Harper and Row, 1974), p. 11.

5. *Ibid.*, p. 15.

6. *Ibid.*, p. 107.

7. *Ibid.*, p. 191.

8. David Kahn, *The Codebreakers (Los descifradores)*, (New York: Macmillan Co., 1967), p. 67.

9. Winterbotham, p. 85.

10. Kahn, p. 591.

11. *Ibid.*, p. 392.

12. Thomas Whiteside, "Dead Souls in the Computer" (Almas muertas en la computadora), *The New Yorker*, 29 de agosto de 1977, pág. 59-62.

13. Tom Alexander, "Waiting for the Great Computer Rip-off" (Esperando el gran timo de la computadora), *Fortune*, Julio de 1974, p. 143.

14. Bonnie Ginzburg, "Military Computers Easily Penetrable, AF Study Finds" (Computadoras militares fácilmente penetrables, averiguaciones de un estudio de la FA), *Washington Post*, 8 de agosto de 1976, p. A6.

15. En agosto de 1976, el Mando de Sistemas de la Fuerza Aérea dirigió la terminación del Programa de Seguridad del Sistema de ADP de la División de Sistemas Electrónicos. La terminación se completó en septiembre de 1977, deteniendo el desarrollo (que iba bien) de un prototipo general seguro para demostrar completamente la aceptabilidad operacional y el desarrollo asociado de especificaciones, recomendaciones de política y criterios de evaluación para uso general.

16. Lawrence Curran, "Air Force 'Kernel' Attains Computer Security Using Existing Technology" (El 'núcleo' de la Fuerza Aérea logra la seguridad de las computadoras usando una tecnología existente), *Electronics*, 30 de septiembre de 1976, pág. 59, 61.

17. El autor hizo una hipótesis inicial sobre el concepto de núcleo de seguridad y su base matemática. La investigación patrocinada de forma subsiguiente en la MITRE Corporation completa la formulación detallada, según se describe en *1976 Computer Security Developments Summary (Resumen de desarrollo de seguridad de computadoras de 1976)* de ESD, MCI-76—2, División de Sistemas Electrónicos, Base de la Fuerza Aérea Hanscom, Massachusetts, enero de 1977.

18. W. L. Schiller, *The Design and Specification of a Security Kernel for the PDP-11/45 (El diseño y la especificación de un núcleo de seguridad para el PDP-11/45)*, ESD—TR-75-69 (Bedford, Massachusetts: MITRE Corporation, mayo de 1975), p. 9.

19. "Computer Security: A Case of Priorities" (Seguridad de computadoras: un caso de prioridades), *Electronics*, 30 de septiembre de 1976, p. 10.

El progreso tecnológico nos ha proporcionado meramente medios más eficientes para retroceder.

Aldous Huxley

**Teniente Coronel Roger R. Schell, USAF** (Doctorado, Massachusetts Institute of Technology) es un Oficial de Intercambio de USAF/USN como Profesor Asistente de Ciencias Informáticas en la Escuela Naval de Posgraduados, Monterey, California. La mayor parte de su servicio ha sido en desarrollo y adquisiciones de sistemas de armas. Sirvió como ingeniero y gerente de software de computadoras, y durante varios años fue gerente del Programa de Seguridad de Sistemas ADP de la Base de la Fuerza Aérea de Hanscom, Massachusetts. Se graduó de la Escuela Superior de Comando y Estado Mayor y de la Escuela Superior de Guerra Aérea, Base Aérea Maxwell, Alabama.

# Sun Zi en un Desafío Creativo

COMODORO JOSÉ C. D'ODORICO, FAA-RET.

*El desafío reside en la propuesta de algunas ideas que procuran frustrar con éxito el embate de un agresor que lleva adelante una guerra no convencional contra un gobierno legítimo.*

## Accediendo a un mundo tenebroso

Los pueblos evolucionan y también el modo de hacer la guerra, no importa cuales sean las razones de su estallido. El conflicto engendrado por la crisis se alinea con el afiebrado dinamismo humano y en ese contexto, la contienda salvaje sigue siendo una llaga incurable de la civilización, que no ha podido ser eliminada ni aun por los sacrificados misioneros de la paz. La historia confirma que ningún líder pudo erradicar el enfrentamiento, pero los repetidos fracasos no han llegado a derrotar las expectativas.

En este ensayo que no reclama exclusividad, procuraremos argumentar con las inferencias que se ajustan a la realidad de las crisis actuales. El producto resultante del análisis auspicia el progreso de la investigación posterior e incita el deseo de acrecentar el conocimiento de los antagonismos que se diferencian de los tradicionales. Por eso es importante preservar la identidad de la crisis y sobre todo la verdad explícita. Tampoco hay que permitir que el propósito y las maniobras del ofensor sean camuflados o falseados.

El General chino Sun Zi, también conocido como Sun Tzu,<sup>1</sup> estudió los entretelones de la guerra con extraordinaria prolijidad. Aunque en aquellos años la ética del combate no atraía la atención preferencial de los jefes, este militar reveló una inusitada preocupación por los prisioneros y el soldado raso. Eso explica que parte de sus meditaciones sean magnánimos consejos sobre los combatientes. Puesto que el pensamiento de Sun tiene cualidades dignas de elogio, evocaremos su obra que nos será útil como soporte de las conclusiones que desgranaremos a continuación.

Una revisión ligera de la situación planetaria, nos dice que un alto porcentaje de conflictos modernos corresponde a la categoría de *guerra no convencional* (GNC), aunque hay gobiernos y profesionales de la defensa que no consienten esta categoría. Sin hurgar en los orígenes de tales eventos, encaramos con modestia el desafío de sugerir una contribución estratégica capaz de hacer frente a una coyuntura bélica de baja intensidad, donde el ofensor representa una asociación de intereses espurios. Las protagonistas habituales de este drama son las genéricamente denominadas *amenazas no tradicionales*, representadas entre otras por el *crimen organizado*, el *narcotráfico*, las *guerrillas mercenarias* y las *migraciones invasivas*. La *guerra civil* y la *subversiva*, pertenecientes a la familia de las GNCs, requieren un estudio separado debido a su trascendencia, complejidad y meta.<sup>2</sup>

Tanto la *guerra convencional* (GC) como los heterogéneos formatos turbulentos que confluyen en las GNCs, tienen sus propias originalidades y por consiguiente conviene estudiarlos aisladamente. Entre las múltiples diferencias que dividen a estos conflictos, merece citarse el objetivo del atacante, el uso táctico de ambas fuerzas, los recursos disponibles en cada bando y las respectivas organizaciones operativas.

La opinión pública y oficial ven a las GNCs como la consecuencia dinámica de *amenazas no tradicionales*, pero generalmente las consideran casos de índole policial. Sin embargo, esos conflictos tienen una historia e inserción que excede la sola incumbencia de las fuerzas del orden. Por eso las defensas mejor entrenadas y apegadas a la realidad, están usando medios y tácticas militares para contener a los criminales. Ante esas evidencias, los funcionarios aún remisos co-

mienzan a aceptar discretamente la necesidad de investigar con más perseverancia la totalidad del fenómeno.

Pero entre la GC y los “otros” conflictos, hay más diferencias que las usualmente visibles a simple vista. El desarrollo de una confrontación clásica es inocultable. En cambio, las “otras guerras” usan artimañas para no ser fácilmente captadas por la sociedad. Las pandillas se exponen al público solo cuando atacan o se defienden.

Hay administraciones que para no empañar su imagen política, niegan la existencia de una GNC en el país, pero ninguna declaración por altisonante que sea modifica la realidad que se confirma con hechos. Aunque las agencias oficiales unen sus respectivos talentos para dibujar un escenario soñado por el gobierno, la realidad que lo enmarca presenta la única verdad. Independientemente del criterio oficial, la verdad confirma que las *amenazas no tradicionales* son fuentes de guerras irregulares.<sup>3</sup>

Una sociedad puede ser embaucada por una realidad configurada ex profeso con fines políticos, pero las anomalías siempre aparecerán en la verdad que emerge de la realidad falseada. La realidad fundada con suposiciones y voluntarismo niega una verdad concurrente. Sin embargo, es entendible que un gobierno quiera ofrecer su propia visión de un país exitoso. Por eso es difícil criticar al Estado que quiere presentar a sus gobernados un panorama optimista de la realidad, aunque esté contaminada por la ficción.

Si una crisis empaña la realidad, las autoridades tienden a aislar el sector intoxicado. Cuando el orden político es conmovido por un conflicto que pone en riesgo la seguridad y el bienestar de la nación, el contagio de la realidad interior es inevitable y prescindente de la reacción del gobierno. La identificación de cualquier tipo de guerra que deforma coercitivamente una realidad anterior, es menos importante que el modo de triunfar que seleccione el gobierno, pues esa decisión influirá sobre el futuro del país.

Cualquier GNC, reconocida o no, genera innumerables trastornos institucionales que enmarcan el desempeño del gobierno. Por eso, los funcionarios se esfuerzan para que el fenómeno cause la menor cantidad de distorsiones en la rutina popular. Con ese fin, tratan de consolidar una realidad más amigable con sus objetivos y procuran asociar a los habitantes en la prueba, pero a veces son fantasías que aletargan el ritmo y la eficacia de la defensa.

Como saldo de esta introducción, se puede afirmar que el país que admite la existencia de una GNC y resuelve derrotarla, acumula ventajas comparativas respecto de otro que prefiere forzar una imagen menos dramática pero engañosa de la realidad nacional para hacerla menos ingrata al público. Es una conducta frecuente, aunque el gobierno también puede estar sinceramente convencido que la crisis que soporta no es de carácter bélico.

## Primero, el problema

Sun Zi sabía que la insuficiencia informativa podía causar una catástrofe y por lo tanto lo puntualizó sin retaceo. “Si conoces a tu enemigo y a ti mismo, en cien batallas no correrás peligro. Si desconoces al enemigo pero te conoces a ti mismo, las posibilidades de ganar o perder se nivelan. Si desconoces a tu enemigo y a ti mismo, estarás en peligro en cada batalla”. Estas y otras ideas que se irán exponiendo como el meollo de doctrinas eternas, fueron incorporadas a El Arte de la Guerra<sup>4</sup> para aleccionar sin estridencias pero con claridad a los conductores de la batalla.

El breviario del General chino sigue siendo a la estrategia y la táctica, lo que la Biblia es a la humanidad. La antigüedad de la obra (unos 2.500 años) no parece haber marchitado las deducciones de Sun Zi y por eso continúa siendo un pensador que despierta reverente admiración. El autor de las teorías insiste en su desmenuzamiento porque “la guerra es un asunto de importancia vital para el Estado y es preciso estudiarla a fondo”.

Cuando el gobierno advierte la alteración de la realidad que lo rodea, enfrenta un problema estratégico, el cual debe resolver porque no puede coexistir con una verdad contrahecha. Si un país es asolado por el *crimen organizado*, la vida interna se resiente y clama por la restauración de la normalidad. Ocuparse de esa áspera situación, significa reordenar los factores desquiciados, principalmente de índole ético-moral, que agravan las instituciones y los estamentos sociales.

La población se desconcierta cuando se separa de la realidad que comparte con la administración legal. Al ampliarse las grietas, aumentan las dificultades que atentan contra el ambicionado frente socio-político leal al régimen, como requiere una estructura defensiva sólida. La dirección política siempre quiere ofrecer la impresión –falsa o real– que controla la situación. Sobre esa aspiración, los funcionarios prefieren no dar explicaciones sobre cómo la manejarán y con qué medios. Pero si el gobierno no obtiene la confianza popular, será difícil que el Estado se fortalezca. Sun Zi entendía que ese déficit ponía en riesgo la victoria, “principal objetivo en la guerra”.

Aunque el estratega chino no se inmiscuyó en GNCs como las que hoy existen, concebidas y llevadas a cabo con refinamiento y equipos modernos, probablemente estuvo en contacto con paradigmas rudimentarios que poseían peculiaridades no muy diferentes de las actuales. No obstante, las reglas de empeñamiento, las normas jurídicas internacionales y los derechos humanos, constituían una fantasía inaprensible. No hay que desmerecer la obra de Sun aunque sean citas acuñadas en el pasado, porque siguen teniendo una exitosa afinidad con la estrategia y táctica de nuestros días.

La trama de las GNCs es tan intrincada que demanda el concurso de autoridades experimentadas y diestras, puesto que deben seleccionar criterios estratégicos y normas legales que determinan la organización de la *campaña*. La réplica del Estado a la GNC exigirá un ordenado debate entre funcionarios, políticos y jefes militares, donde todos defenderán sus intereses parroquiales, pero acabarán orquestando un consenso construido sobre una base lógica y la decisión del gobierno.

El comportamiento fluctuante de los guerreros en el combate dio lugar a que Sun concibiera la doctrina de la “responsabilidad colectiva”. En esa teoría, el conductor chino dejó asentado que todos los militares, desde el campesino-soldado hasta el General, tenía una cuota obligatoria de participación en el combate, acorde con el nivel jerárquico. Por lo tanto, cada hombre era sujeto de una supervisión múltiple. Los ineptos y cobardes no debían escapar a los drásticos castigos de entonces y los valientes recibían halagos y botines.

La identificación incorrecta del conflicto es una falla de quien la realiza y comúnmente es causa de esfuerzos excesivos sin una compensación apropiada. Si el General no “basa sus planes en la *configuración* del antagonista”, condición que abarca las maniobras, tácticas y pertrechos empleados por el oponente, el rendimiento de las operaciones decae.<sup>5</sup> Si el gobierno se muestra indiferente a ese error, luego tendrá que soportar consecuencias desagradables. Ignorar la realidad pone en peligro la esencia de la guerra, la victoria, porque cuando la realidad es ignorada, planea su propia venganza.

Los comentarios realizados aquí aspiran a aumentar la comprensión de las novedosas crisis que salpican los albores del corriente siglo. Intereses diversos presionan para que las GNCs sean explicadas como fenómenos de índole social, policial o político corriente, admisibles en un mundo donde no faltan las tensiones. Sin embargo, la interrelación de los elementos que potencian el conflicto muestra una imagen distinta a la promovida por los analistas que recurren a descripciones frecuentadas. Esta conclusión emerge del soporte de una realidad que no siempre es acertadamente interpretada, sobre todo por los inexpertos.

No sabemos si Sun incursionó en contiendas que hoy calificaríamos de GNC, pero el militar chino sí sabía que debía emplear las armas con cordura y sin odio. Por eso aconsejó usarlas solo cuando “el enemigo no puede ser vencido por otros medios, en cuyo caso hay que lograr la victoria en un plazo breve, dosificar los esfuerzos, acotar la pérdida de vidas y tener el menor número de bajas posible”.

Sun Zi sabía que el daño causado por las armas es letal. Por lo tanto, las consideraba “instrumentos ominosos que solo deben usarse cuando no hay otra alternativa” y además agregaba, “el aniquilamiento del enemigo, la destrucción de las ciudades y la devastación de los campos, no deben constituir objetivos militares”. La misma exhortación cabe en las contiendas actuales y exige acuerdos durante las operaciones.

## Decisión + Voluntad = Victoria

Después de incursionar en el problema como primer paso del plan, el segundo es menos exigente. Pero no tiene sentido hacer un examen puntilloso de la dificultad si más tarde el producto es condenado a la inmovilidad, destino que no se debe descartar. Entre las causas frecuentes de ese comportamiento citamos el abandono oficial, la incredulidad, la escasez de recursos, ausencia de jefes con iniciativa, un acompañamiento popular retaceado, pugna de tendencias opuestas y un marcado déficit informativo sobre el adversario.

De los vicios antes indicados, el más nocivo y tal vez más usual es el *laissez faire* que prevalece en los regímenes frívolos y populistas, inundados de funcionarios deshonestos, corruptos e ineptos. No hacer nada, hacerlo mal o hacerlo sin una finalidad loable, son procedimientos contrarios a una buena defensa. El agresor acumula ventajas cuando gana la iniciativa y con ella logra más libertad de acción. Así podrá hacer “la aproximación indirecta al objetivo”, una táctica muy atractiva. Mientras, Sun consideraba que antes había que asegurar “la unidad nacional como requisito esencial para ganar la guerra”.

Según Clausewitz,<sup>6</sup> vencer en la guerra equivale a doblegar la voluntad del contrincante, pero esa meta exige que previamente el liderazgo político haya afirmado la decisión de producirla. La voluntad es acopio de energía potencial que se pone en movimiento con el impulso que le entrega la decisión de vencer. La confluencia de las partes que colaboran con el Estado depende de la pericia socio-política demostrada por el gobierno, aunque siga habiendo ciudadanos que no distinguen el avance de la guerra heterodoxa.

Cuando el gobierno comienza la *campaña* contra una *amenaza no convencional* con el único sostén de sus capacidades, queda expuesto a riesgos innecesarios que no radican en la calidad de la decisión de vencer. Proviene de un enemigo cuyas artes no tienen restricciones ético-morales y sus reglas de empeñamiento no respetan condicionantes de ningún tipo. En ese TO (teatro de operaciones) tan turbulento, los contendientes acuden a menudo a su intuición, pero el triunfo empieza a cuajar con el apoyo de la sociedad.

Sun Zi estudió con esmero la influencia que tiene la condición anímica de las tropas, por considerarla un factor importante en la victoria. Por eso aseveró que “el estado de ánimo enemigo es un blanco prioritario y deteriorarlo es un paso previo al encuentro armado”. Un oponente bien plantado debe ser desgastado psicológicamente “con anticipación al combate” para que el choque sea menos duro. Según Sun, un General experto “solo ataca cuando la situación asegura la victoria, por lo cual su misión debe componer esa realidad”.

## La integración de la *campaña*

No hay que comenzar una *campaña* sin comprender que la guerra es un “asunto de importancia vital para el Estado y debe ser estudiada a fondo”, aunque sea un LIC (low intensity conflict) interno. No es un consejo superfluo, ni una obviedad, por lo cual Sun Zi analizó acabadamente la importancia que el fenómeno bélico representaba en la vida socio-política del Estado y sus conclusiones intervinieron en la especulación estratégica.

En un evento trastornante como la guerra, el gobierno tiene una enorme responsabilidad que no puede ejercer sin contar con la cooperación mutua de todas las agencias estatales. En un ré-

gimen democrático es fundamental obtener la ayuda concertada de los poderes que lo integran, o de lo contrario la infiltración enemiga se hará notar en las instituciones como excrescencias de la realidad. Es una ventaja indeseada que no hay por qué donar gratuitamente al bando hostil. Si el poder ejecutivo (PE) inicia la *campaña* sin el respaldo de los restantes sectores nacionales, la unidad interior se parecerá a una fantasía.

Una vez que el gobierno recoge el guante del contendiente ilegal, la integración de la unidad interna es prioritaria y previa a la *campaña*. Sun instruyó con frases sin artilugios a los directores de la *campaña*. “El objeto de la guerra es la victoria y no hay que alargar las operaciones aunque sean maravillosamente conducidas, pues ningún país se beneficia con una guerra prolongada”. Como el ofensor tal vez planea desarrollar un conflicto de largo aliento, el defensor tiene que intentar acortarlo. Por eso el consejo de Sun apunta al fracaso de la *estrategia sin tiempo*,<sup>7</sup> que se suele utilizar en las GNCs.

Los tres poderes del Estado democrático [PE, legislativo (PL) y judicial (PJ)], con la dirección del PE, combinan las funciones con el fin de restaurar la paz y el orden. La decisión de imponer la voluntad oficial a una corporación delincencial, se materializa con leyes internas. Los otros dos poderes, desde sus respectivos feudos profesionales, tienen que secundar las fórmulas acordadas con el PE en cumplimiento del plan de *campaña*.

Quienes supongan que la GNC es un modelo de contienda convencional en escala reducida, tal vez imaginen que el alistamiento para la defensa será amplio y oneroso. Pero es común que la GNC adquiriera el formato de un LIC<sup>8</sup> doméstico menor. Los acontecimientos bélicos de alto voltaje son menos frecuentes y se producen cuando los sediciosos tienen número suficiente para operar indistintamente en ciudades y zonas rurales.

Durante una GNC, la rutina social no suele hacer cambios extraordinarios en los hábitos populares. En estos conflictos intervienen unidades con menor poder de fuego, la contribución aérea y naval es secundaria pues se hace a requerimiento, las fuerzas legales y el adversario se mezclan en el mismo TO, los actores se confunden con delincuentes vulgares y la logística del ofensor imita el comercio regular.

Las levedades mencionadas no impiden que la GNC se parangone con la teoría de la guerra,<sup>9</sup> aunque su presentación visual difiera de la GC. Los factores más diferenciados de ambas contiendas son el objetivo y la consecuencia social del evento. El beneficio de la iniciativa hace que el agresor imponga su arte combativo y el Estado no puede quedar ajeno a la desagradable realidad que lo apremia. La inspiración defensiva lo llevará a trazar planes que se encarguen de “evitar el daño y obtener las ventajas”<sup>10</sup>.

Una defensa que supone que la delincuencia doméstica solo trasgrede las leyes del país, es arquitectónicamente débil para hacer frente a una GNC en acecho y no advierte que está en el umbral de un enfrentamiento de mayor entidad. La apreciación distorsionada de la realidad, induce la utilización de equipos y criterios tácticos que normalmente el Estado emplea con fines menores. Si el PE no percibe esa *gaffe*, las consecuencias no tardarán en llamarle groseramente la atención.

Colombia, México y Brasil están luchando en indiscutibles GNCs y a ese fin llevan a cabo *campañas* de diferentes envergaduras contra el *narcotráfico* y las *guerrillas mercenarias*, comandados por el *crimen organizado*. Las estrategias en curso procuran la eliminación de las bandas y los resultados reflejan la eficiencia lograda. Otros Estados, como Perú y Bolivia, se atienen a pautas defensivas menos estables y más ocasionales. El 12 febrero 2012, el Ejército peruano capturó a Florindo Flores (a) *Artemio*, jefe operativo de Sendero Luminoso y dos secuaces, anotándose un éxito local importante.

Ampliando lo dicho, observamos que el gobierno de Colombia optó por hacer uso de una actitud ofensiva liderada por las FF.AA. y emplea la policía como fuerza complementaria. En ese país, la GNC es parte de la realidad nacional. En México, el gobierno utiliza una modalidad de-

fensiva, donde la policía es prioritaria. La idea de la guerra no ha encarnado en el estamento político y el Estado usa recursos civiles con refuerzos militares.

Sin embargo, los millares de muertos registrados en México debido a este conflicto, ameritan una revisión calificadora de la situación. En Brasil, la policía militarizada está a cargo del rol ofensivo y las operaciones de envergadura reciben apoyo militar. La GNC está inserta en la realidad, pero el gobierno se abstiene de considerarla una contienda.

Sun Zi observó que las guerras tenían sus propias excentricidades, por lo cual el sentido común le indicó que “la adaptación a la situación es un punto importante en el examen y por lo tanto es preciso ser flexible”. Una vez que la misión es asignada por el PE, el comandante “debe basar sus planes en la *configuración*<sup>11</sup> del adversario” y debe “evaluar la situación antes de marchar, correr riesgos solamente estudiados y evitar los innecesarios”.

Cuando los tres poderes del Estado hacen converger su funcionamiento con la realidad, la *configuración* de la víctima es menos favorable para el agresor. Para revertir la situación, los delincuentes cometen toda clase de tropelías y actos *terroristas*, desorientando a los inexpertos. Los facciosos usan el *terror* sin cortapisas, como método coercitivo de efecto paralizante instantáneo. Tampoco descartan las artimañas que producen daños morales y menoscaban la imagen pública de burócratas y personas respetadas. Esta práctica operativa es reforzada con desinformación y propaganda (PSYOPS, operaciones psicológicas).

El victimario culpa a la víctima de su conducta deshonesta, intentando demoler la reputación de las autoridades. Los asesinos se auto nominan perseguidos políticos; custodios de los derechos populares y sociales, y acusan a la legítima defensa nacional de abusar del poder. La *contra campaña* del ofensor recurre a un enjambre de insidias, reproches e imputaciones falsas sobre el gobierno.

Por estas y otras razones, cuando el gobierno es desafiado con una GNC dinamizada por la corporación criminal, se perfila la aparición de una realidad diferente. El ofensor trata de mantener viva esa falacia porque la defensa se endurecerá si la descubren. También difundirá que sus procedimientos se ubican en el ámbito jurídico-policial y por lo tanto se auto asigna el derecho de protestar por el empleo de órganos defensivos más contundentes.

Los poderes estatales, guiados por el PE, tienen que diseñar una plataforma legislativa y jurídica que legitime las responsabilidades defensivas. Sun Zi, solo con una frase y con arreglo a la lógica, enunció esa delicada definición diciendo, “el ejército no se puede dirigir con normas de la etiqueta; la benevolencia y la rectitud se practican en el gobierno de un Estado, pero no en la conducción del ejército”. La enunciación de Sun se fundó en dos pilares indiscutibles y tan antiguos como las FF.AA.: jerarquía y disciplina.

Siempre hay que darle a las fuerzas nacionales una cobertura jurídica legal que las preserve de la ignominiosa intencionalidad criminal. Para inhibir la interferencia seudo jurídica de los delincuentes, el PE necesita el soporte y complemento de los otros poderes del Estado que le dan contenido al apotegma “la unión hace la fuerza”<sup>12</sup>. Para atenuar el estrés que genera una GNC, el defensor necesita saber que su compromiso y vocación están amparados contra el cinismo de la corporación, que no tiene contrición para acudir a los procedimientos más condenables. Las reglas de empeñamiento del *crimen organizado* ratifican esa diagnosis. El entorpecimiento de los organismos oficiales atrasa el avance de los planes y operaciones, a la vez que aumenta el costo de la defensa.

Cuando el adversario obstruye el funcionamiento del Congreso y del sistema jurídico, exterioriza indirectamente que la defensa oficial está bien encaminada, pues así demuestra que ambas instituciones le causan un daño que necesita terminar. Conseguir que todas las dependencias estatales trabajen armónicamente en el desarrollo de los planes, tal vez constituya una esperanza utópica, pero el beneficio expectable merece que la administración haga una prueba con ese fin.

## La estrategia, un desafío al ingenio

El PE es responsable de bosquejar la estrategia para dismantelar el cartel ilegal que amenaza la paz interior. Mientras funcionarios idóneos conciben con ese fin la maniobra general en función “del engaño y la impostura” recomendados por Sun Zi como principio de la ciencia militar, hay otros sectores que mencionan a diversas agencias estatales como también dedicadas a preservar el orden y la seguridad. Esa cita puede ser una observación sincera, pero igualmente puede enmascarar otras intenciones.

El ejemplo mencionado no es extraño y eventualmente le da algunas ventajas a los ilegales. El ciudadano común, informado a medias o que no está interesado en lo que acontece, probablemente crea que esos organismos de bajo perfil le darán la seguridad que anhela. Pero si realmente estuvieran destinados a mantener la tranquilidad pública, estarán preparados para combatir la delincuencia común que es menos aguerrida que el *crimen organizado*. Asimismo, cuando el gobierno se equivoca al identificar el conflicto, el alistamiento puede tener fallas.

No hay que ligar las líneas estratégicas a criterios ortodoxos porque la crisis se caracteriza por su inestabilidad. Las singularidades del conflicto se localizan en la configuración del TO, la doctrina ambigua y los modos de empleo. Por eso, en la GNC se usan equipos usuales y particulares. Además de los rasgos subrayados, hay discordancias en las reglas de empeñamiento, donde los defensores tienen que demostrar cuánto conocen sobre la interioridad del conflicto.

Por lo expresado previamente y al tener cada GNC una identidad funcional, proponer un modelo estandarizado de estrategia para conducir cualquier conflicto es absurdo. Los delincuentes se mueven con habilidad en los laberintos urbanos y son tácticos duchos, obligando a que la defensa emita planes de calidad. En estas coyunturas, los comandos avezados eligen pautas estratégicas ajustadas a las características de la GNC en curso.

Al insinuarse una GNC, es normal que por un lapso haya un vacío informativo que obstaculice el cálculo de su duración y el conocimiento de los pormenores. Las instituciones estatales están habituadas a los planes que definen sus fases con el tiempo-almanaque o del reloj. En cambio, los delincuentes eluden esa tiranía y se adecuan a la consecución de los objetivos (*estrategia sin tiempo*). Ninguna defensa establecerá una estrategia acertada con un enunciado abstracto basado en una realidad indefinible y tampoco puede jurar que retornará a sus cuarteles únicamente después de conquistar el objetivo propuesto.

Toda estrategia oficial tiene una línea de partida que es el comienzo de la *campana*. La GNC es una variante de la *guerra prolongada* que prospera con la *estrategia sin tiempo*<sup>13</sup>. Estos dos factores son capitales en las secuencias a devenir y deben ser tomados en cuenta por el PE cuando elija la forma de ganar la guerra. El gobierno atacado por un adversario no convencional, no siempre individualiza con acierto el peligro que corre. El error surge de las conductas equívocas, las excesivas formalidades, cortesías vinculares y relaciones políticas engoladas, pero las actitudes de ese tenor no tienen buena cabida en una GNC.

El PE debe encargarse de la conducción del plan de defensa consensuado por un comité nacional y con fines ejecutivos designará un comando conjunto cívico-militar, compuesto por funcionarios expertos en *amenazas no tradicionales*, que deben operar con criterio *net-centric*<sup>14</sup>. El conocimiento es un requisito insoslayable porque los profesionales sin capacitación en GNC, ponen en riesgo la *campana*. Si “la unidad nacional es un requerimiento esencial para ganar la guerra”, también lo es el conocimiento de sus características.

El comando conjunto de defensa tiene que recibir la jurisdicción territorial nacional porque la sectorización fragmenta las decisiones y da lugar a los grupos que velan más sus intereses que la universalidad del objetivo. Tales circunstancias engendran duplicaciones, gastos extras y debates que atrasan las decisiones. Aunque el diálogo político es beneficioso, es contrario a la rapidez y reduce la ventaja de la iniciativa.

En la GNC, el enemigo trabaja para que la sociedad no se solidarice con las políticas oficiales. El escenario legal óptimo se configura cuando los tres poderes estatales aceptan la realidad y se alejan de los espejismos. Al mismo tiempo, la defensa de la nación se afirma cuando la comunidad se encolumna espontáneamente detrás de las autoridades nacionales, encomiando la verdad que deviene de la realidad. No hay que olvidar que la realidad ignorada, planea su propia venganza.

Coincidentemente con la selección de los pilares de la estrategia, el PE debe convocar a los otros poderes estatales para hacer acuerdos indispensables. En primer lugar, apurar las normas que agravan los delitos cometidos por el ofensor y cubren la intervención legal de las fuerzas del orden. Luego, convenir con el PJ el acortamiento de los juicios incoados durante la GNC para promover sentencias perentorias con trámites sumarios. La concertación de los tres poderes valoriza la eficacia de la defensa.

## La información del pueblo

Cuando la vida social es alterada por un LIC, la comunidad desea saber más sobre la realidad de la que es parte. Sin embargo, no siempre la información pública es difundida con equilibrio. Los sucesos nacionales influyen en el ánimo popular y sus efectos motivan el interés de los técnicos en comunicación social del comando de defensa. Si los medios son controlados por los delincuentes, el gobierno estará en desventaja.

Es normal que el libre acceso a la información sea protegido por las instituciones. Pero cuando una GNC conmueve la paz interior, hay que revisar con prolijidad las obligaciones y derechos de la sociedad. El acto de informar y ser informado se transforma en un dilema con premisas opuestas, cuyos contenidos retienen el interés de las partes. La libertad informativa es aprovechada por personas inconsideradas que rápidamente la convierten en un sucio libertinaje.

El *crimen organizado* no auto impone fronteras al uso de la libertad para sus fines. Por lo tanto, el gobierno tiene que evitar que un derecho que no es absoluto, ponga en peligro a las instituciones y la comunidad, o sea, debe reglamentar la libertad informativa para impedir que los delincuentes se beneficien con esa prerrogativa. Si un órgano de prensa colabora con la corporación revelando un secreto de la defensa, viola reglas de seguridad y su acto es punible. Luego el Congreso tiene que emitir disposiciones que resguarden ese interés nacional.

Por supuesto, no es el único *modus operandi* del *crimen organizado*. Es usual que la información destinada al público sobre la realidad nacional, siga una vía descendente con destino a la conciencia colectiva de la multitud, intentando modelar culturalmente los estamentos populares. El valor socio-político de esa circulación crece cuando el pueblo recibe del gobierno la información deseada. Por eso las PSYOPS tienen que ser manipuladas por agencias especializadas y solo una emergencia justificaría que el comando conjunto se ocupe por sí solo de esa tarea.

Es común que la situación cambie erráticamente, pero la comunidad tarda poco en adaptarse a las nuevas condiciones. No obstante, todo cambio interno tiene que ser estudiado para que los planes defensivos confronten adecuadamente cada aspecto del desafío. Si el pueblo no está satisfecho con el liderazgo oficial, la armonía se vuelve intratable y el gobierno tiene que introducir las correcciones aconsejables. Las encuestas periódicas de opinión, generan datos ascendentes de gran valor para los escalones superiores del gobierno y aun para el comando operativo.

Sun Zi, un agudo analista de la realidad, enunció numerosas y oportunas nociones doctrinarias sobre los conflictos. Uno de los tantos pensamientos se apoya en la sencillez de su comprensión y nunca debe ser olvidado: “la vulnerabilidad depende del enemigo, la invencibilidad, de uno mismo; lo que depende de mí, puedo controlarlo, pero lo que depende del enemigo, no estoy seguro. Uno puede aprender cómo ganar, pero no necesariamente sabe cómo conseguirlo.”

## El entorno socio-económico

Cualquier líder medianamente experimentado supondrá que si un país se encuentra en una GNC *prolongada* con reglas de la *estrategia sin tiempo*, tiene que adecuarse a esa realidad. El desprecio de la verdad por el Estado favorecería la aparición de problemas políticos y defensivos que lo pondrían al borde de un desenlace desastroso. Este cuadro inseguro y complejo demanda una respuesta franca a una pregunta inexorable, ¿saben las autoridades cómo conducir un LIC interior, presuntamente de larga duración, sin permitir que el fenómeno haga peligrar el progreso nacional?

Si las respuestas se dieran a conocer, tal vez la sorpresa sería mayúscula, pero los gobiernos marginan sus flaquezas. En este sentido, Sun subrayó que, “cuando el ejército se pone en movimiento, los precios se elevan; cuando los precios aumentan, la riqueza del pueblo disminuye”. Sun se refirió primitivamente a la inflación y la corrosión económica que causa. Esa condición es una carga pesada para los menos favorecidos, pero también impone su efecto en el sistema logístico de la defensa.

En la GNC, el pueblo parece un actor de reparto en una obra fantástica. A lo largo de la guerra, la conducción está obligada a investigar las inquietudes populares, las tendencias políticas y las esperanzas de la sociedad. Esos datos y el producto de las encuestas, deben ser enviados al comando de defensa para aumentar la información. Durante la crisis, es importante contar con la cooperación de los partidos políticos del país, porque sus cuadros tienen un constante contacto directo con la población.

Si el gobierno consigue más libertad de acción durante la guerra, es porque el pueblo confía en sus dirigentes. Tal condición permite que la administración dedique más atención al conflicto. En un ambiente socio-político ordenado, las instituciones obran con menos inconvenientes y transmiten tranquilidad al pueblo. Es un contexto positivo para la defensa legal y por consiguiente la neutralización de los criminales es menos complicada. En ese ambiente, el aparato productivo recupera ritmo y confianza, que es un coeficiente colateral vitalizador de la defensa.

Cuando el *crimen organizado* convulsiona un Estado, el PE debe aplicar de manera inelástica las leyes vigentes. Este criterio incluye la contribución del PL y el PJ, mediante procedimientos desarrollados en paralelo. Cuando el gobierno aplica sin vacilar y con firmeza la legislación destinada a refrenar la *amenaza no tradicional*, el éxito no tardará en llegar. La *campana* contra el enemigo abarca a los cómplices, clandestinos o no. Durante ese período es preferible que las autoridades usen procedimientos lo menos cruentos posible para no sobrecargar a la sociedad ni exacerbar a la prensa, pero no deben titubear cuando sea indispensable. No hay que confundir medida con timidez.

El plan de *campana* debe desarrollarse con las mejores fuerzas para ese tipo de operaciones, pero esta norma no siempre es acatada. Al mismo tiempo, el comando debe supervisar que no se produzcan *daños colaterales* o procurar que sean insignificantes. De ese modo se evitará que las reglas de empeñamiento oficiales no sean criticadas, ni la corporación ilegal tenga fundamentos para censurar la defensa. El gobierno atrae la simpatía popular cuando la prensa más respetada lo respalda y denuncia a la organización criminal.

Las operaciones programadas por el comando conjunto tienen que ser ejecutadas con circunspección y tacto para no alarmar inútilmente a la civilidad. Las fuerzas insuficientes o pobremente adiestradas son propensas a ser derrotadas y no confían en sí mismas. Sun dio la impresión de adelantarse a su época al aconsejar, “usar las fuerzas militares solamente cuando el enemigo no puede ser vencido por otros medios, tratar de lograr la victoria en el más breve lapso y con la menor pérdida de vidas, invertir esfuerzos moderados y tratar de infligir el menor número de bajas”. También dijo que la cantidad no es determinante, “pues recibe la influencia de la calidad, disciplina, administración justa y entrenamiento”.

El poder político debe reclamar el respaldo del pueblo para que la *campana* demande un esfuerzo menor. Ese auxilio se logra con la colaboración de especialistas en el manejo de grupos humanos. La GNC es normalmente de larga duración, pero tiende a abreviarse cuando el gobierno gana la colaboración social. Para hacer fracasar al Estado, los criminales apelan a diversas variantes del *terror*.

El *terrorismo*<sup>15</sup> es un método extremo que tiene afinidad con el *crimen organizado* y por lo tanto lo utiliza en concordancia con sus objetivos. Esa trastada exenta de impedimentos morales, produce una presión salvaje sobre entidades y personas a las que la delincuencia quiere someter por el miedo, destruir psicológicamente o simplemente eliminar. Si el Estado no piensa dejarse vencer por la corporación, la represión del *terrorismo* exige una réplica categórica e inmediata que confirme esa decisión.

El *terrorismo*, cruento o incruento, resquebraja la rutina social y causa enormes dificultades al gobierno por la inseguridad que genera. La defensa nunca alcanza para proteger a todos los objetivos existentes en el TO y aunque el gobierno es responsable de reducir a los asesinos, el ciudadano común tiene que brindar toda la ayuda que pueda sin incluir el uso de armas y el riesgo de su vida.

Cuando el desasosiego aparece en la comunidad, los habitantes se amedrentan y somatizan el peligro que emerge de la actividad delictiva. Al mismo tiempo, la economía se resiente debido al ánimo menguante de los trabajadores y la declinación se aprecia en la producción, el comercio y la rutina urbana. Cuando el *terror* aumenta, el miedo esclaviza al pueblo y la ayuda voluntaria contra los delincuentes decae visiblemente.

Aunque la sociedad sea el blanco de toda clase de agresiones, es probable que siga sin darse cuenta que está en medio de una GNC, por cuanto el evento es confundido con brotes más despiadados de delincuencia. El público que desconoce la realidad, piensa que estos episodios pueden ser neutralizados con fuerzas policiales más numerosas. Aunque el gobierno y la gran mayoría de la población consideren que la alteración de la paz ciudadana es un asunto de pura índole cívico-policial, los analistas profesionales contemplan otra verdad.

Si la sociedad no identifica correctamente la naturaleza del conflicto, el Estado no debe considerarse exculpado y está obligado a llegar al fondo de la realidad antes de proponer una réplica acorde contra el agresor. El desenlace llega cuando el comando recibe una misión destinada a obtener la victoria. El plan concurrente evidenciará una estrategia adecuada a la realidad y la *campana* expondrá el desarrollo matricial de la historia. La lacónica arquitectura de esta solución defensiva, se instrumenta según Sun Zi bajo la guía del dogma clásico de la ciencia militar: “el engaño y la impostura”.

Contrariamente a la guerra tradicional, la GNC se nutre con una cantidad minoritaria de reservistas. La mayoría de los convocados se destinan a las unidades terrestres después de cumplir un período de entrenamiento MOUT (Military Operations in Urban Terrain), aunque es probable que también haya necesidad de técnicos para atender sistemas y equipos avanzados.

## Presupuesto y equipos

Nunca hay que comenzar una *campana* sin contar con un presupuesto que la financie, aunque hay que saber que “el país se empobrece con las operaciones militares” y por lo tanto, “cuando el ejército se pone en marcha, la tesorería del país debe estar bien provista”. Las autoridades deben estar conscientes que si el ejército “se involucra en campañas prolongadas, los recursos del Estado no alcanzan”. Para Sun Zi, era imprescindible que en las contiendas de duración incierta, no se interrumpieran las operaciones.

En una GNC se pueden utilizar parcialmente los recursos disponibles para la GC. Cada elemento evaluado debe superar el filtro del sentido común, el costo y las características de la gue-

rra. Como la confrontación usual de este tipo es *prolongada*, el objetivo del atacante suele carecer de restricción calendaria y es fijada por la consecución. Cuando la GNC se alarga, el presupuesto y el cálculo de los recursos debe someterse a revisiones periódicas, tomando en cuenta el principio de economía en el empleo.

Una frase de Sun Zi recuerda que “la victoria es el principal motivo de la guerra”. La sentencia suena a perogrullada, pero la recordación no es ociosa porque hay casos en que los contendientes abandonan la lucha antes de conseguir el objetivo deseado. Son decisiones políticas de los actores, pero las contradicciones chocan con las previsiones determinadas por la crisis y a veces, veladamente, encubren la sombra de una derrota.

Para que un gobierno no tenga que modificar el fin natural de una *campaña*, debe responder a la realidad, cuidar el gasto y supervisar celosamente la evolución de los hechos. El gobierno debe prepararse para atender la demanda de insumos que reclama la GNC, aunque a priori desconoce cuantas unidades militares tendrá que emplear. La situación siempre tiene su reflejo en el cálculo financiero y si el gasto se descontrola, el pueblo se empobrece. Para Sun Zi, este segmento de la realidad era un axioma empírico.

Solo un líder poco reflexivo se adelantará a elegir los sistemas de armas que utilizará en una GNC que aún desconoce. Es una improvisación, porque cada conflicto plantea su propia realidad. Solo una cantidad limitada de material convencional es aprovechable en el LIC. Los sistemas se deducen de la topografía, las tácticas enemigas y el aporte que pueden hacer los centros abastecedores, pero es el gobierno el que dice cómo la política, economía e industrias intervendrán en el circuito logístico.

Las prestaciones de los sistemas de armas modernos cautivan a los profesionales que, aun sin una apropiada experiencia y estudios, desean su adquisición. Pero la administración tiene que contener esos impulsos para que el gasto de la defensa no convierta el presupuesto en un problema nacional. No hay que olvidar que la seguridad y bienestar del pueblo son metas políticas principales de cualquier gobierno democrático.

Aunque para Sun el colmo de la pericia es “someter al enemigo sin librar combate”, el atacante no es dócil y hay corporaciones que se animan a desafiar a los gobiernos enclenques. En los enfrentamientos de baja intensidad, los UAS/UCAS (unmanned aerial system/unmanned combat aerial system) cumplen un papel destacado en el reconocimiento y fuego aéreo cercano (CAS), pero no todos los países pueden adquirirlos y operarlos.

Sun Zi también señaló que “un principio de la guerra dice que el enemigo avanzará y hay que estar listo para enfrentarlo. No se debe suponer que no atacará y por lo tanto tenemos que ser invencibles”. El General chino remató su observación indicando que “la rapidez es esencial en la guerra, en tanto que la imprevisión del enemigo es una ventaja”. En esa línea de pensamiento, hay que emplear los sistemas de armas más aptos para cada contienda.

La velocidad abrevia el tiempo de reacción y urge al rival. Hoy la industria ofrece sistemas de efectos instantáneos que obliga a los contendientes a recurrir a planes esquemáticos y sin escrupulos retóricos. Cuando un Estado Mayor cumple su tarea, es probable que ninguno de sus miembros esté informado que el marqués Wu Zi se refirió con una refinada lógica al plan como el arte de la victoria. Por eso, si el Estado retiene una hipótesis de guerra que le permite hacer previsiones confiables, la sorpresa tiende a diluirse.

Cuando hay indicios indiscutibles que la GNC es dirigida por el *crimen organizado*, el gobierno debe alertar a la defensa y ordenar medidas preliminares. Es importante que los funcionarios no confundan la crisis que avanza con el recrudecimiento del crimen en una gran urbe. Por eso es conveniente despejar las ambigüedades, cotejando un LIC interno y la acción delictiva ordinaria. La identificación certera de la dificultad orienta el estilo de la defensa, el cálculo inicial de los recursos y una estructura orgánica conveniente.

Siendo la GNC una variedad de LIC, el principio de economía en el empleo de los medios es una condición *sine qua non* que requiere atención durante todo el pleito. El alargamiento inde-

finido de la disputa deja su rastro en la economía nacional y por eso hay que seleccionar sistemas de armas de bajo costo y mantenimiento sencillo, descartando las sofisticaciones tecnológicas onerosas. Paralelamente hay que evaluar detenidamente las ofertas de los fabricantes que entusiasman a los profesionales.

Para contribuir a montar un escenario calmo aunque el país esté a punto de involucrarse en una GNC, la defensa debe actuar sin estridencias ni exageraciones. La vigilancia territorial, el rastillaje de las zonas infectadas por los trasgresores y su captura, tienen que efectuarse sin alboroto para no alarmar al pueblo y electrizar a la prensa con hechos indebidamente ostentosos.

El entorno geográfico más frecuentado por el *crimen organizado* es el urbano, donde ciudadanos y facciosos entran en contacto aun sin concienciarse de esa realidad. En la ciudad, las personas se informan de modo muy dispar. Por eso la defensa tiene que ser hábil y rápida para proteger a los ciudadanos y reprimir al rival. En ese TO se emplean armas livianas, de precisión y elementos no letales. Los vehículos blindados de gran poder de fuego, la artillería y casi toda la munición aérea, son raramente utilizados.

En zonas muy edificadas se necesitan comunicaciones satelitales para asegurar el enlace continuo, vital en las tácticas urbanas. La exploración con UAS es ventajosa, en tanto que el traslado de personal y carga se efectúa con helicópteros, APCs (Armoured Personnel Carrier) y vehículos MRAP (Mine Resistant-Ambush Protected) protegidos contra los IEDs (Improvised Explosive Device). Actualmente hay sistemas aéreos de detección sobre aeronaves C-IED (Counter-IED) B200 King Air, Dash 8 y Twin Otter, y variados modelos de UAS<sup>16</sup>. En el espacio abierto, se pueden usar sistemas convencionales.

El principio de economía en el empleo de medios también se aplica en la determinación del número de combatientes, teniendo como límite la referencia aconsejada por la doctrina (7/10:1 promedio). No obstante, “las fuerzas no son numéricamente decisivas”, puesto que la eficiencia depende de factores, como “la calidad, disciplina, administración y entrenamiento”. Las tropas sugeridas para intervenir en una GNC son las Fuerzas Especiales con instrucción MOUT y reglas de empeñamiento concordantes.

Cuando estas unidades se desplazan en lugares públicos, atraen una atención limitada de los observadores y no generan la inquietud que produce una columna blindada. Los civiles menos informados hasta pueden confundirlas con formaciones policiales de infantería, que son menos preocupantes para los ciudadanos corrientes.

## Conclusión

El espíritu de Sun Zi, relacionado con la teoría de la GNC, se percibe en la arquitectura estratégica del conflicto y desnuda sus afinidades con la moraleja de Aristóteles,<sup>17</sup> el griego, que demostró que la realidad es la única verdad. La lógica de la verdad, antes de convencer a Aristóteles, iluminó a Sun Zi para clarificar las respuestas a los interrogantes más espinosos sobre el hecho bélico, considerado como un fenómeno socio-político-militar que determina la evolución de una nación.

La intervención de Sun fue tan perspicaz como proficua, por lo cual sus especulaciones no solo lo prestigiaron. Futuros e ignotos colegas usufructuaron más tarde las deducciones contenidas en las recomendaciones del General. La obra de Sun fue atesorada en un documento<sup>18</sup> que sigue proyectando la sabiduría de sus sentencias sobre nuestro juicio y desde ese pedestal doctrinario, el militar chino escapó a la opacidad que exuda el tiempo. No obstante y es justo decirlo, algunos estudiosos del arte militar creen que en ese legado no hay “nada nuevo bajo el sol” (Eclesiastés 1.9).

Para quienes las critican o las celebran, las introspecciones de Sun Zi están disponibles para todos aquellos que se animen a desafiarlas sin abusar de extravagancias discursivas que sepultan

las deducciones lógicas. Por supuesto, los capítulos del Arte de la Guerra requieren extrapolaciones que no olviden la historia del conflicto y de la tecnología. Los estrategas que cuestionan a Sun Zi, estiman que sus ideas han sido superadas por la modernidad. Sin embargo, esa opinión está teñida de voluntarismo, pues la simbiosis objetiva de las ideas de Sun y las GNCs actuales, derrumba tales afirmaciones.

A pesar de las opiniones críticas de aquellos que piensan distinto a Sun Zi, sus consejos siguen siendo útiles y válidos en todos los tipos de confrontaciones, aun de aquéllas a las que los gobiernos se resisten a considerar como una guerra. Las manifestaciones del General chino tienen el implícito y discreto auxilio de la lógica, y esa es una protección que difícilmente puede ser dejada de lado. Los gobiernos y pueblos que se ven envueltos compulsivamente en episodios internos y transnacionales de tono bélico, tal vez de volumen reducido pero bélico al fin, son pruebas vivas de las visiones de Sun.

El uso del “velo y engaño” actual, equivale al “engaño y la impostura” cultivados por Sun. A primera vista, parecen recursos vituperables, pero nadie ha dejado de aprovechar sus excelencias desde tiempo inmemorial para transformarlas en prácticas ocurrentes y astutas, sin dar importancia a los reproches y cuestionamientos ético-morales. Los artificios que anidan en el “engaño y la impostura”, dan sustento a las reglas de empeñamiento de las GNC, y aumentan la flexibilidad y eficiencia que proporciona la iniciativa. Los que aseguran que 2.500 años aminoraron el valor de las deducciones de Sun, no ignoran que los militares utilizan las doctrinas fundadoras para encaminar nuevas realizaciones.

Hoy, cuando hay tantos países angustiados por las consecuencias de las siniestras GNCs, los organismos de defensa debieran prestar más atención a la erudición de Sun Zi. Su código para la guerra, contiene originalidades que merecen ser pareadas con la realidad que nos rodea. Por lo tanto, este colofón no finaliza aquí, además reclama el ahondamiento del conocimiento y la proyección de las GNCs, a las que aún no se les acredita la importancia que tienen. Si las defensas siguen relegando el estudio de estos conflictos, el mundo continuará enlutándose asombrado y se extraviará en la búsqueda de soluciones escurridizas. □

#### Notas

1. Este General habría vivido en los años 500 a.C., pero sus escritos militares siguen siendo una fuente de sabiduría para los estrategas y tácticos, porque conceptualmente conservan plena frescura. Se considera que El Arte de la Guerra es su obra cumbre.

2. El volumen político del conflicto no determina la clasificación.

3. Com.FAA José C. D’Odorico, ret., La Guerra y los Protagonistas, en La Guerra No Convencional, *Air & Space Power Journal*, español, ediciones de 2010 a 2012.

4. El Arte de la Guerra, atribuido a Sun Zi, consta de 13 capítulos que contienen clarividentes recomendaciones a gobernantes, estrategas y tácticos comprometidos en una crisis bélica.

5. En adelante, todas las frases colocadas entre comillas, corresponderán al pensamiento de Sun Zi, salvo aclaraciones contrarias.

6. General Carl von Clausewitz (1780-1831), autor De La Guerra, ocho volúmenes sobre teoría, estrategia y filosofía del fenómeno bélico.

7. Com. FAA J.C. D’Odorico, ret., El Tiempo, Incordio de la Estrategia, *Air & Space Power Journal*, español, 1° trimestre 2010. Además, ídem 3.

8. El conflicto de baja intensidad demanda una participación parcial de las capacidades del país, puesto que por lo general, el oponente no tiene aptitud para poner en peligro la estabilidad del Estado.

9. Com. FAA J.C. D’Odorico, ret., La Guerra No Convencional, ídem 3.

10. Un pensamiento del marqués Wu Zi, contemporáneo de Sun Zi.

11. Ya vimos que Sun Zi sintetiza así las cualidades, capacidades y decisiones del oponente.

12. Autor desconocido.

13. Com.FAA J.C. D’Odorico, ret., El Tiempo, Incordio de la Estrategia, *Air & Space Power Journal*, español, 1° trimestre 2010. Además, ídem 3.

14. Maximización del potencial de un sistema de sistemas, en el cual se fomenta la relación entre nodos complementarios (bases, sensores, centros, unidades) para incrementar sus respectivos rendimientos.
15. Com.FAA J.C.D'Odorico, ret., ídem 3. Ver El Terrorismo en la Guerra Irregular, ASPJ, español, II trimestre 2011.
16. IHS Jane's Defence Weekly, 15 Feb.2012, vol. 49, # 07.
17. Aristóteles, 384-322 a.C.
18. El Arte de la Guerra, citado anteriormente.

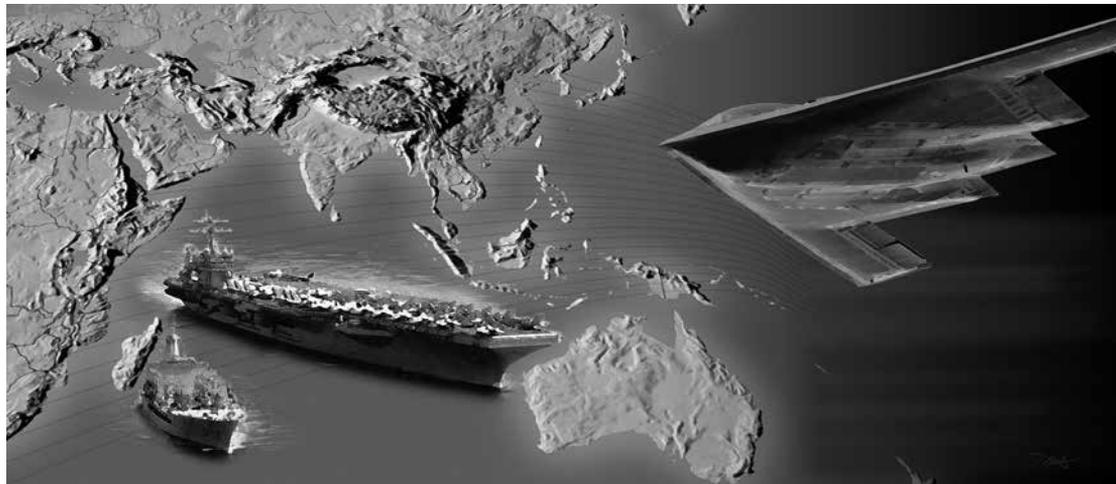


**El Comodoro (R) José C. D'Odorico**, Fuerza Aérea Argentina (FAA), fue piloto de transporte aéreo con más de 5.000 hrs de vuelo, habiéndose retirado del servicio activo en 1975. Se especializó en el estudio de la guerra revolucionaria marxista-leninista y la guerra subversiva. Es autor de tres libros y más de 350 artículos profesionales, algunos de los cuales fueron publicados en *Air University Review* y *Air & Space Power Journal*. Actualmente se desempeña como Asesor de la *Revista de la Escuela Superior de Guerra Aérea* (RESGA).



# El Factor Australiano en la Estrategia del Pacífico Occidental de los Estados Unidos

LIAO KAI



**R**ECIENTEMENTE, las disputas relativas al Mar del Sur de China (MSC) han pasado al primer plano del interés mundial. Estados Unidos ha hecho múltiples esfuerzos para influenciar los desacuerdos chino-filipino y chino-vietnamita. En numerosas ocasiones, los líderes políticos y militares estadounidenses han expresado su decisión de defender los intereses estadounidenses en la esfera de influencia del Pacífico Occidental. De igual manera, los militares estadounidenses han realizado con sus aliados de Asia-Pacífico, incluyendo ex enemigos, en una serie de ejercicios militares conjuntos. China se opone enérgicamente a cualquier intento de internacionalizar las disputas del MSC y quiere llegar a acuerdos mediante esfuerzos bilaterales. China considera la entrada de Estados Unidos en esta disputa como un desafío a sus intereses e interferencia con asuntos territoriales y de relaciones exteriores de China. Aunque no ha establecido claramente su posición en el problema del MSC, Australia envió tropas a un ejercicio militar conjunto con Estados Unidos y Japón en el MSC en julio de 2010. Más recientemente, Australia permitió que una fuerza de Infantería de Marina estadounidense utilice permanentemente una de sus bases costeras del norte. Es posible que China interprete todos estos desarrollos como actos de ayudar a Estados Unidos en estrechar las “cadenas de islas”.

Este artículo identifica brevemente el panorama estratégico alrededor y más allá del MSC, discute el concepto de Batalla AireMar de los Estados Unidos, y después ofrece un análisis detallado del factor australiano en este concepto y los retos que representa para China. Finalmente, el artículo propone un curso de acción que China puede tomar para manejar la cambiante situación del MSC.

## Intereses de China en el Mar del Sur de China

Para predecir la evolución de las disputas del MSC, se debe entender cómo las ve China, dónde están sus intereses, y si tales intereses son generales o básicos por naturaleza. En primer

lugar, China reclama soberanía sobre las aguas del MSC y de las islas Nansha (Spratly). Sin embargo, los estados vecinos rivales no han apoyado este reclamo. De hecho, los desacuerdos en soberanía sobre el MSC han existido por muchos años. Después del descubrimiento de una enorme reserva de recursos estratégicos bajo las aguas del MSC, esta controversia aumentó su volatilidad. Segundo, las Islas Nansha flanquean el paso de China al Océano Índico a través del Estrecho de Malaca. Aquí la ramificación es doble: (1) Económicamente, el comercio chino depende en gran medida de esta vía marítima de comunicaciones. Específicamente, cerca de la mitad del petróleo crudo que importa China pasa por Malaca. (2) Estratégicamente, si estalla el conflicto —en particular, si se bloquea el Estrecho de Malaca— China perdería una considerable parte de su suministro de energía y también sus exportaciones globales, lo que a su vez estrangularía el desarrollo sostenido de China. Finalmente, el MSC forma un eslabón de la llamada primera cadena de islas del litoral de China. No romper esta cadena impedirá la libertad de acceso al Océano Índico y al Pacífico Sur. Según el *Washington Post*, Dai Bingguo, consejero estatal de China, describió el MSC como parte del “interés nacional fundamental” de China en su reunión con la Secretaria de Estado de los Estados Unidos, Hillary Clinton, en mayo de 2010.<sup>1</sup> No se pudo hallar confirmación de este reporte en ningún medio oficial chino, pero no hay duda que el MSC toca intereses fundamentales de China. En otra ocasión, el Almirante Michael Mullen, ex presidente del Estado Mayor Conjunto de los Estados Unidos, escuchó a su contraparte chino, General Chen Bingde, jefe del Comando General del Ejército de Liberación Popular (ELP), decir que “China, junto con los países vecinos, tiene la sabiduría y la capacidad para manejar adecuadamente las disputas del MSC. Estas disputas no necesitan la participación de Estados Unidos mucho menos que se preocupe de ello”.<sup>2</sup> Obviamente, el General Chen le estaba diciendo a Estados Unidos que no meta sus narices en las disputas del MSC.

## Intereses estadounidenses en el Mar del Sur de China y su posible intervención

Ignorando las reiteradas advertencias de China, Estados Unidos está decidido a mantenerse involucrado en las disputas del MSC —un curso de acción que China considera que solo complicará la situación, escalándola más que aliviándola. ¿Cuáles son los intereses de Estados Unidos en la controversia del MSC o su solución? ¿En qué formas permanecerá involucrado?

Los militares estadounidenses y los grupos de expertos consideran que el MSC es vital para los intereses estadounidenses en el Pacífico Occidental.<sup>3</sup> En su visita a Hanoi en 2010, la Secretaria de Estado Clinton señaló que “Estados Unidos. . . tiene un interés nacional en la libertad de navegación, acceso libre a las vías marítimas comunes de Asia, y el respeto por la ley internacional en el Mar del Sur de China”.<sup>4</sup> Sin embargo, China siempre ha interpretado lo que Estados Unidos considera “libertad de navegación” como “libertad de espionaje”, en virtud de la cual sus militares pueden maniobrar libremente a lo largo de la costa de China para reunir inteligencia y vigilar sus actividades terrestres y aéreas. Igualmente, en base al argumento de defender esta libertad de navegación, Estados Unidos y sus aliados están formando primeras y segundas cadenas de islas cada vez más estrechas. Para contener la expansión de China en el Pacífico Occidental, en el transcurso de los años, el gobierno estadounidense y sus militares han perfeccionado progresivamente sus estrategias, la más reciente y sistemática de las cuales es la Batalla AireMar. La instalación oficial de la Oficina de Batalla AireMar dentro del Pentágono el 9 de noviembre de 2011 marcó el último avance de convertir este concepto en una realidad.

## Perspectiva de China de la Batalla AireMar

China ha podido sostener su impulso de crecimiento desde la reforma económica de 1978. Su poderío nacional continúa expandiéndose, al igual que su poderío militar. Recientemente, China pasó a ocupar el segundo lugar en el mundo en términos de gastos militares. Fortalecida por su creciente poder económico y militar, China está más segura de poder manejar los asuntos de política exterior internacional y su propia defensa nacional. Como desarrollo lógico, China ha definido —y ampliado— sus intereses nacionales, junto con una estrategia de defensa más activa. Siguiendo estas líneas, China ha participado en la patrulla y escolta de convoyes en el Golfo de Adén y en actividades de mantenimiento de la paz de las Naciones Unidas. Igualmente notable es el hecho de que China está mejorando rápidamente su flota de superficie y submarina en cantidad y calidad, y actualizando sus misiles balísticos antibuque, evidenciado por el modelo más reciente el DF-21D. Tales esfuerzos son ampliamente interpretados como el aumento de la capacidad de disuasión de China y de su capacidad antiacceso y negación de área (A2/AD) en el Pacífico Occidental. Como se podía esperar, la única superpotencia actual siente la presión y le preocupa la inminente injerencia en sus intereses nacionales a lo largo de la periferia de China y en el mar. Los militares estadounidenses creen que el ELP está preparado para amenazar la libertad de acción estadounidense en varios frentes. Específicamente, las bases militares estadounidenses en Japón y Guam ya no son seguras; las fuerzas estadounidenses podrían no ser capaces de contener a las fuerzas del ELP en áreas del Pacífico Occidental; y para los activos de comando y control y de reconocimiento espacial sobre el Pacífico Occidental también existe el peligro de ataque.<sup>5</sup> Para disuadir y derrotar a China en el Pacífico Occidental, Estados Unidos ha propuesto varias estrategias para contrarrestar la capacidad A2/AD.

Entre ellas, el concepto de Batalla AireMar —supuestamente desarrollado primero por el Centro para Evaluaciones Estratégicas y Presupuestarias— atrajo la mayor parte de la atención. Eventualmente, los militares estadounidenses adoptaron las ideas del concepto, y los aliados asiáticos clave la apoyaron. Esta estrategia supone que durante un conflicto entre China y EE.UU. en el Pacífico Occidental, las fuerzas del ELP tendrían capacidad A2/AD para atacar las bases estadounidenses en Guam y Japón, lanzar una guerra de información total, y destruir los “oídos y ojos” de las fuerzas estadounidenses mediante misiles antisatélite y ciberataques—el llamado la maza del asesino. Después de estudiar la maza del asesino del ELP y prestarse del concepto de Batalla AireMar desarrollado por los militares estadounidenses en la década de 1980, los estrategas estadounidenses formularon la Batalla AireMar, que supone combinar las fuerzas aéreas y marítimas en una fuerza coherente y utilizar a los aliados asiáticos en funciones importantes. Específicamente, la primera fase de las operaciones militares estadounidenses incluiría ganar y sostener la iniciativa durante la primera ola de ataques preventivos del ELP. En la fase siguiente de operaciones convencionales, los militares estadounidenses “cegarían” rápidamente los sistemas de información y comunicación de las fuerzas adversarias para frustrar los esfuerzos A2/AD. La Batalla AireMar sigue este curso de acción:

- Cegar al oponente.
- Defender las bases y activos militares de defensa prioritaria.
- Suprimir las fuerzas de misiles balísticos y crucero de medio alcance basados en tierra del ELP.
- Atacar los sistemas de comando y control, vigilancia de área amplia y defensa aérea del ELP
- Atacar las capacidades de superficie y subterráneas del ELP.
- Ejercer gran presión sobre la economía, sociedad y liderazgo chinos.<sup>6</sup>

En mayo de 2012, el Secretario de Defensa Robert Gates señaló que “el acuerdo de la Marina y la Fuerza Aérea para trabajar juntos en un concepto Batalla AireMar es un evento prometedor,

que tiene el potencial de hacer para el poderío disuasivo militar de Estados Unidos al comienzo del siglo 21 lo que la Batalla Aire Tierra hizo hacia el final del siglo 20”.<sup>7</sup> En octubre de 2010, en una reunión anual de los funcionarios de relaciones exteriores y defensa australianos y estadounidenses, Gates prometió reforzar el despliegue militar estadounidense en Australia y aumentar los vínculos de defensa entre ambos países.<sup>8</sup> Apenas un año después, estos dos países anunciaron que Australia proporcionaría una base permanente en su costa norte para una fuerza de Infantería de Marina de los Estados Unidos.<sup>9</sup>

## Estrategia de defensa australiana y su función en la Batalla AireMar

Descendientes de las mismas raíces anglosajonas, Australia y Estados Unidos comparten muchas identidades culturales e ideológicas. Australia ha sido por mucho tiempo un aliado clave en la región Asia-Pacífico bajo el tratado ANZUS (Australia-Nueva Zelanda-Estados Unidos) firmado hace casi 60 años. En todas las guerras iniciadas o luchadas por Estados Unidos fuera de sus bordes, Australia ofreció apoyo incondicional. Más aún, los australianos atribuyen la paz en la región durante las últimas décadas a la fuerza de estabilización proporcionada por Estados Unidos. A cambio, el Presidente George W. Bush en 2003 saludó a Australia como su “sheriff” en Asia del Sureste.<sup>10</sup> Tales vínculos estrechos entre estas dos naciones hacen que China preste mucha atención a la orientación estratégica de Australia. Aunque China y Australia no presentan amenazas directas entre ellos y no tienen conflictos de interés, de algún modo Australia considera a China como una amenaza potencial a su seguridad nacional; además, China siente desconfianza del ANZUS y se pregunta cómo reaccionaría Australia ante conflictos potenciales entre China y Estados Unidos. Indudablemente China entiende que en cualquier conflicto futuro entre China y EE.UU., la actitud de Australia será importante. Ignorando el escrutinio de China, Australia se identifica reiteradamente como un aliado cercano de los Estados Unidos. Por ejemplo, durante un discurso en el Brookings Institution en 2010, Stephen Smith, Ministro de Defensa australiano, aseguró nuevamente a la audiencia que “Australia es un aliado que añade valor. No somos un consumidor de seguridad de Estados Unidos que impone decisiones difíciles sobre los militares y la política pública de Estados Unidos”. Sin embargo, Smith terminó su discurso diciendo con indignación, “Agregamos valor y lo hacemos desde un punto de vista de respeto, no de dependencia.”<sup>11</sup> De esta declaración, se podría inferir que Australia desea actuar como un estado independiente con políticas de relaciones exteriores y de seguridad independientes —no como seguidor ciego de los Estados Unidos. Australia elige alinearse con Estados Unidos por sus propios intereses nacionales. Entonces, ¿cómo ve Australia a China desde su perspectiva estratégica y de defensa independiente? ¿Y cómo afecta a China el factor australiano, o la función que desempeñe —desde el punto de vista geoestratégico y militar?

Como lo sugiere el título de su documento de investigación de defensa de 2009, *Defensa de Australia en el Siglo de Asia Pacífico: Fuerza 2030*, Australia es consciente de que el futuro de su panorama estratégico será afectado por la distribución global y regional del poder político, económico y militar; la transformación de las relaciones de las grandes potencias en la región Asia Pacífico, especialmente el surgimiento de China; y sus relaciones con Estados Unidos.<sup>12</sup> Económicamente, China es el socio comercial número uno de Australia. En otras palabras, la economía australiana está estrechamente vinculada a esta relación comercial. Desde el comienzo del siglo veintiuno, Australia ha disfrutado un mercado de exportación muy fuerte en oro, carbón, mineral de hierro, y muchos otros recursos, gracias en gran parte al rápido desarrollo económico y la creciente demanda de recursos de China. Sin embargo, hay brechas importantes entre estos dos países en muchas áreas, especialmente en cultura y sistemas políticos. Tales brechas se han ampliado en los últimos dos años a raíz del arresto en China de empleados de Río Tinto, una empresa minera británico-australiana, acusados de corrupción y espionaje. La desconfianza se

profundizó más después de las revelaciones de WikiLeaks que el ex premier australiano Kevin Rudd supuestamente dijo a la Secretaria de Estado Clinton “que esté preparada para usar la fuerza contra China”.<sup>13</sup> En términos de territorio marítimo, Australia es ciertamente una de las naciones más grandes del mundo; por lo tanto, la libertad de los mares es importantísima para la economía y seguridad de Australia. Proclamando jurisdicción sobre 27,2 millones de kilómetros cuadrados (la mitad de los cuales “sobre el océano o el mar”) o 5 por ciento del planeta, Australia debe defender y expandir sus intereses nacionales a través del mar.<sup>14</sup> Un país con enormes reservas de recursos naturales, a Australia solo le faltan agua y población —vulnerabilidades inherentes que la vuelven una potencia comparativamente débil económica, política y militarmente. En consecuencia, los australianos no parecen estar muy seguros de su propia capacidad para defender el vasto territorio y recursos que controlan.

En claro contraste, China es un país superpoblado, ávido por recursos y no muy lejos de Australia. Por tanto, los australianos vigilantes no pueden dejar de preocuparse que algún día en el futuro, cuando China gane libertad de acción en el MSC, pueda expandirse más hacia el sur acercándose a Australia, y presentar una amenaza más inminente a su seguridad nacional. Una encuesta revela que el 55 por ciento de los australianos consideran que China es la potencia económica más importante del mundo. Mientras tanto, 57 por ciento cree que “el gobierno australiano está permitiendo demasiada inversión de China”. En otras palabras, la mayoría de australianos están preocupados con la ola de inversiones chinas. Cuarenta y cuatro por ciento de ellos piensa que “China se convertirá en una amenaza militar para Australia en los próximos 20 años” mientras que el 55 por ciento no está de acuerdo.<sup>15</sup> Aunque muchos analistas australianos entienden la importancia de China para la economía y el comercio australiano, así como para el antiterrorismo global, cuando se discute el surgimiento de China, quedan más preocupados.

Podemos ver que económicamente Australia ya está interrelacionada con China, pero en el nivel psicológico, su gente está dividida en relación a sus sentimientos hacia los chinos. Geológicamente, Australia está situado donde el Océano Índico se encuentra con el Pacífico Occidental. La línea costera noroccidental de Australia casi toca el borde del Océano Índico, más allá del cual está el MSC. Al establecer una base conjunta o combinada estadounidense en Australia, Estados Unidos gana otra base de avanzada. Esta base, comparada con las de Hawaii, facilita la logística en el caso de un conflicto en el MSC. Igualmente importante, comparada con Japón y Guam, Australia está fuera del alcance de la mayoría de misiles de lanzamiento por tierra o mar del ELP. La base australiana no solo facilita la operación de las fuerzas estadounidenses desplegadas en los conflictos del MSC sino que también juega un papel importante en los potenciales conflictos en el Océano Índico. Su ubicación estratégica, profundidad en tierra, afinidad natural con los Estados Unidos, y la sospecha psicológica sobre China, hacen que Australia sea un aliado ideal de Estados Unidos. En la estrategia estadounidense para el Pacífico Occidental y el Océano Índico y, en particular, para tratar con China, la alianza Australia-Estados Unidos se hará más estrecha e importante. En su libro *AirSea Battle (Batalla AireMar)* (2010), Jan van Tol establece claramente que “*La Batalla AireMar no es un concepto únicamente estadounidense*. Países aliados como Japón y Australia, y posiblemente otros, deben desempeñar roles habilitadores importantes para sostener un equilibrio militar estable” (énfasis en el original).<sup>16</sup> En esta Batalla AireMar propuesta, se espera que Australia proporcione a Estados Unidos profundidad estratégica, participe en ganar el dominio del mar, apoye a las fuerzas estadounidenses en sus operaciones en el Océano Índico Oriental y en el MSC, y asista desviando algunos ataques del ELP.

Si estallara un conflicto entre China y Estados Unidos, es probable que el comercio de China con Estados Unidos y Japón se reduzca dramáticamente. Los militares estadounidenses se concentrarían en cortar el comercio de China con el mundo exterior, incluyendo la estrangulación de Malaca y algunos otros estrechos dentro de territorio de Indonesia, para impedir que China navegue hacia el Océano Índico. El bloqueo del Estrecho de Malaca, una tarea no muy difícil para los militares estadounidenses, obligaría a China a cambiar la ruta de su línea de transporte

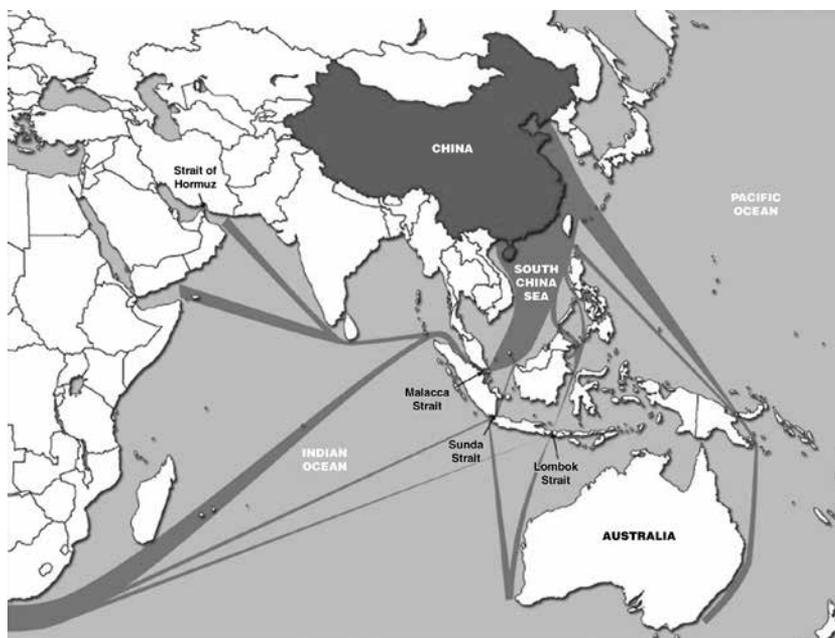
hacia el sur a través del Estrecho de Sonda y el Estrecho de Lombok, ambos situados hacia el noroeste de Australia (ver la figura siguiente). Los lectores minuciosos podrán encontrar en el documento de investigación de defensa de 2009, mencionado anteriormente, que Australia intensificó sus medidas de seguridad. Aunque su enfoque anterior buscaba asegurar territorio desde el mar solamente, los líderes militares australianos han adoptado ahora una estrategia de doble negación que incluye capacidades de negación marítima y aérea. Además, el ámbito estratégico de Australia se ha expandido hacia el Océano Índico oriental.<sup>17</sup>

Muchos influyentes analistas de defensa australianos elogian el concepto de Batalla AireMar. Las publicaciones de los investigadores militares y de defensa de Australia en los últimos dos años coinciden con ese método de defensa del país, revelando que está intensificando la preparación militar para una Batalla AireMar coordinada. Por ejemplo, el documento de investigación de defensa de 2009 establece claramente que en los próximos años Australia reforzará su capacidad militar. Específicamente, el gobierno australiano “ha prometido un crecimiento real en el presupuesto de defensa de 3 por ciento hasta 2017–18 y 2,2 por ciento de crecimiento real en adelante hasta 2030.”<sup>18</sup> En el año 2010, los gastos militares de Australia alcanzaron un nuevo máximo de 24 mil millones de dólares americanos, pasando a ser el número 13 en el mundo.<sup>19</sup> El profesor Ross Babbage, un asesor en ese documento de investigación de defensa, sugiere también que, además de los ataques militares, los estados aliados deben iniciar una “campaña anti-comercial generalizada” contra China. Tal acción interrumpiría las transacciones comerciales y monetarias de China, estrangulando su acceso a energía y materias primas de Europa y Oriente Medio y, si fuera necesario, interceptar sus flotas “en lugares distantes, como en los estrechos marítimos de Asia del Sureste”. Predice que esto “produciría daño grave a la economía china y, de hecho, riesgos fundamentales para la élite gobernante misma”.<sup>20</sup> Aunque esta predicción por sí misma merece serios cuestionamientos y aunque la economía australiana sufriría enormemente debido a estas acciones, el punto de vista de Babbage sugiere que el concepto de Batalla AireMar, junto con su hostilidad oculta contra China, está ganando el apoyo de los aliados asiáticos de Estados Unidos.

Australia nunca ha aclarado su posición en el posible conflicto entre EE.UU. y China. Por un lado, Australia ha expresado su preocupación sobre la expansión de China, como se menciona explícitamente en su documento de investigación de defensa de 2009.<sup>21</sup> Igualmente, en el comunicado conjunto de las Consultas Ministeriales entre Australia y Estados Unidos firmada por funcionarios de defensa estadounidenses y australianos en noviembre de 2010, las dos naciones se comprometen a una cooperación más estrecha en los dominios del mar, aire, espacio y ciberespacio. Australia permitirá más instalaciones estadounidenses en su territorio y permitirá que Estados Unidos utilice más puertos, bases y otras instalaciones.<sup>22</sup> El Ministro de Defensa Australiano confirmó que en junio de 2010, un equipo especial de la Fuerza Aérea de los Estados Unidos llegó a Australia del norte para estudiar la “base súper secreta Harold E. Holt de Exmouth” para posible expansión de la “vigilancia de satélites y submarinos chinos”.<sup>23</sup> Por otro lado, cuando se le preguntó sobre las circunstancias en que “Australia podría decir no a Estados Unidos en el caso de alguna clase de situación militar en Asia del Este o Asia-Pacífico”, el Ministro de Defensa Smith respondió, “Dejé en claro en mi discurso que Australia estuvo hombro a hombro con Estados Unidos en todo conflicto en que Estados Unidos ha participado desde la Segunda Guerra Mundial. . . . Pero en cada ocasión que tomamos la decisión de entrar en un conflicto, lo hicimos en base a lo que consideramos que debe ser el interés nacional y el interés de seguridad de Australia”.<sup>24</sup>

Además, el documento de investigación de defensa de Australia de 2009 adopta una posición similar sobre este tema: “El gobierno reconoce que Australia puede y debe desempeñar su parte en asistir a Estados Unidos al tratar las amenazas a la seguridad global y regional. . . . Sin embargo, nunca nos debemos poner en una posición donde el precio de nuestra propia seguridad sea un requisito para poner tropas australianas en riesgo en teatros de guerra distantes donde no

tenemos intereses directos en juego”.<sup>25</sup> Por lo tanto, como lo indica este documento de política, Australia aún discute estratégicamente el curso a seguir. Los australianos aún se preguntan si el país debe continuar dependiendo de Estados Unidos para la estabilidad y seguridad regional y qué debe hacer Australia para fortalecer su propia capacidad de defensa y desarrollar una fuerza autosuficiente moderna. Los australianos sospechan de China, y en algunos casos les disgusta. No obstante, también están muy conscientes de que la importancia de China para la economía australiana es cada vez mayor.



**Figura. Líneas marítimas de comunicación de China.** (Adaptado de Jan van Tol con Mark Gunzinger, Andrew Krepinevich, y Jim Thomas, *AirSea Battle: A Point-of-Departure Operational Concept (Batalla AireMar: Un Concepto Operativo de Punto de Partida)* [Washington, DC: Centro para Evaluaciones Estratégicas y Presupuestarias, 2010], <http://www.csbaonline.org/wp-content/uploads/2010/05/2010.05.18-AirSea-Battle.pdf>.)

Surge otro dilema del deseo del gobierno australiano de permanecer hombro a hombro con Estados Unidos aunque no esté seguro si este hermano mayor seguirá manteniendo el dominio del Pacífico Occidental en los 20 próximos años. Igualmente, el gobierno australiano desea fortalecer su cooperación militar con Estados Unidos, pero enfrenta dos obstáculos. Primero, casi la mitad de la población se opone a una presencia militar estadounidense importante en su suelo (55 por ciento apoya y 43 por ciento se opone, mientras que el 20 por ciento apoya enfáticamente y 22 por ciento se opone enfáticamente).<sup>26</sup> Segundo, el Partido Laborista gobernante actual parece menos entusiasta en permitir que las tropas estadounidenses permanezcan en Australia. Ese país puede elegir apoyar a China y Estados Unidos en la transformación conjunta del orden regional, o puede decidir ayudar a que Estados Unidos siga siendo la potencia dominante. De cualquier forma, su decisión tendrá enormes consecuencias estratégicas para China y Estados Unidos, y para la región. Considerando todo esto, China debe prestar mucha atención a las tendencias dentro de la estrategia de defensa australiana y al desarrollo de la cooperación militar entre Australia y EE.UU.

## Sugerencias para los elementos decisorios de China

Este artículo sugiere que los elementos decisorios chinos usen un enfoque de tres fases — corto plazo, mediano plazo, y largo plazo— para mitigar los desafíos estratégicos que encuentra China en el Pacífico Occidental.

### *Corto plazo*

Primero, China debe abstenerse de tomar medidas que puedan causar tensiones que desaten conflictos militares sobre el MSC. Entretanto, China debe persistir en resolver las disputas del MSC a través de negociaciones bilaterales, en lugar de multilaterales, y en todos los casos impedir la internacionalización de estos desacuerdos. Así como no interfiere con los asuntos internos de otras naciones, China no debe permitir que un tercero se entrometa en cualquier consulta bilateral entre ella y los vecinos rivales sobre disputas territoriales. Las tendencias recientes indican que Estados Unidos o algún miembro de la Asociación de Naciones de Asia del Sureste (ASEAN) podría proponer una negociación bilateral entre la ASEAN y China o una negociación de varias partes con la participación estadounidense. Si estuviera presionada por estas propuestas, China debe tratar de desviar la presión a través de canales económicos y diplomáticos. Por ejemplo, China podría animar a más estados amigables de la ASEAN (Myanmar, Camboya, etc.) para que presenten contrapropuestas. Además, usando todos los medios económicos y diplomáticos necesarios, China deberá tratar de persuadir a Australia para que mantenga su cooperación militar con Estados Unidos dentro de un ámbito apropiado, sin llegar a ser parte de la Batalla AireMar. El hecho de que Australia consintió recientemente “un aumento importante de la presencia de Infantes de Marina de los Estados Unidos en rotación en las Barracas Robertson de Australia” parece indicar que Australia ha decidido asociarse con Estados Unidos en la Batalla AireMar diseñada presumiblemente contra China.<sup>27</sup> Estando ya en un estado pasivo, China debería hacer el mejor uso de la garantía de Australia de que una alianza militar entre Australia y EE.UU. no tenga a China como objetivo. Además, China debería proponer o aceptar propuestas sobre ejercicios militares conjuntos con Australia, como un gesto de buena voluntad y un medio de frenar cualquier acción militar contra China.

### *Mediano plazo*

China debe preparar una estrategia de mediano y largo plazo desde una perspectiva que se oponga a la Batalla AireMar. Por ejemplo, “la acción de cegar”, mencionada reiteradamente en el concepto de Batalla AireMar, es supuestamente la táctica favorita de los militares estadounidenses para ganar la iniciativa. Para contrarrestar este intento, el ELP debería aumentar la protección de su red de informaciones y comunicaciones, junto con copias de respaldo redundantes. El hacerlo asegurará que el ELP podrá resistir la primera ola de ataques sin que le “cieguen” los ojos. Además, el bloqueo de la Armada Real Británica durante la Primera Guerra Mundial puede inspirar a las fuerzas estadounidenses a cortar la línea de transporte marítimo de China “con miras a ejercer mayor tensión sobre la economía china y, eventualmente, tensión interna”.<sup>28</sup> Para contrarrestar esta acción, China deberá mejorar sus relaciones con los países de Asia Central para obtener el suministro garantizado de petróleo y gas. Además, China podría reconstruir la “ruta de la seda” (una ruta a lo largo de la cual China inició comercio con países de Asia Central y del Sur en el siglo uno), convirtiéndola en una “línea de comunicación terrestre” importante o un patio trasero protegido. Algo más importante, China debería continuar su alianza estrecha con Myanmar y Paquistán. Este enfoque amplio disolverá efectivamente cualquier “tensión interna” causada por el bloqueo marítimo. De hecho, China ha estado ejecutando esta estrategia previsoramente y ha logrado gran avance. En las últimas tres décadas, no ha dejado de desarrollar cooperación económica con los estados de Asia Central, Paquistán y Myanmar, construyendo

ferrocarriles y carreteras que atraviesan fronteras y tendiendo oleoductos y gasoductos. La actual relación profundamente fracturada entre Paquistán y Estados Unidos a raíz del asesinato de Osama bin Laden y, más recientemente, de dos docenas de miembros del servicio militar paquistaní por helicópteros y aviones de la Organización del Tratado del Atlántico Norte ha abierto otra oportunidad única para China.<sup>29</sup> Aprovechando esta oportunidad y llenando el vacío, los líderes chinos pueden mantener este aliado tradicional más firmemente de su lado.

### *Largo plazo*

China debe continuar activamente su participación en las operaciones auspiciadas por organizaciones internacionales. Además, siguiendo el ejemplo de Estados Unidos, a través de actividades de mantenimiento de la paz, antiterrorismo, antipiratería, y socorro humanitario, el ELP puede obtener valiosa experiencia en operaciones de ultramar, esencial para el fortalecimiento de sus poderíos marítimo y aéreo. China puede también explorar la crisis económica global actual, alquilando y restaurando puertos extranjeros en puntos estratégicos así como aumentando la cooperación militar con estados tradicionalmente amigables. Un caso reciente involucró una propuesta para establecer una base para combatir la piratería en Seychelles. China puede también introducir a otras naciones, como Indonesia, Mauricio y Fiji en su cálculo ayudándolos económicamente y considerando cómo desarrollar cooperación militar con ellos, posiblemente construyendo una base naval o una instalación de inteligencia, vigilancia y reconocimiento en algún momento. En resumen, China debe tener una línea marítima de comunicaciones protegida (la llamada collar de perlas) desde el MSC hasta el Océano Índico. Analizando exhaustivamente las fortalezas y vulnerabilidades de las fuerzas estadounidenses, y maximizando sus propias ventajas, China puede evitar la derrota en un conflicto futuro.

En algún grado, el estado de vigilancia australiana hacia China es instigado por la adquisición agresiva de recursos de su país que hace ésta. Desviando sus inversiones en recursos a otras regiones y países, China podría disfrutar del beneficio doble de (1) mitigar el riesgo de depender demasiado de solo unas cuantas fuentes de suministro y (2) hacer que naciones como Australia entiendan que los intereses nacionales son a menudo recíprocos. China debe dedicar un esfuerzo igual a desarrollar confianza mutua y reducir la sospecha a través de diálogo e intercambio cultural más frecuente. Como se sugiere en el discurso del ministro de defensa australiano en Brookings Institution y en el documento de investigación de defensa australiano de 2009, China debe aumentar la “apertura y transparencia” en relación a capacidades y la doctrina estratégica.<sup>30</sup> China debe tender la mano, participar, y explicar persuasivamente el propósito de su creciente presupuesto de defensa para establecer confianza mutua y apaciguar las preocupaciones de sus vecinos, cercanos y distantes. Así como Australia se prepara para la transformación estratégica de décadas de duración en Asia, China tendrá que adoptar una estrategia de largo plazo que comprometa a Australia por un lado y, por el otro, haga que Australia esté plenamente enterado que China sigue muy de cerca su preparación estratégica y cooperación militar con Estados Unidos.

Para mantener la concordia con los países de Asia del Sur, China deberá continuar usando su capacidad económica —incluyendo plataformas cooperativas y consultivas regionales o bilaterales— con el fin de desarrollar mecanismos de prevención de conflicto. La Organización Cooperativa de Shanghai sirve como un buen modelo que China puede emplear en establecer medios similares para resolver varias disputas. Además, a través de medios diplomáticos explícitos, China debe cerciorarse de que sus vecinos entiendan claramente sus valores e intereses fundamentales y que no se deben inmiscuir en ellos. Al mismo tiempo, China (como siempre lo ha hecho) debe mantener su determinación de defender sus valores e intereses fundamentales por todos los medios viables, incluyendo la fuerza si es necesario. China no tiene que preocuparse demasiado por comentarios negativos sobre los aumentos en su presupuesto de defensa. Un presupuesto de

defensa de aproximadamente 2 por ciento del producto interno bruto (PIB) nacional es en realidad pequeño, especialmente cuando se mide el gasto per cápita o se compara al presupuesto gigante de defensa de Estados Unidos. En los próximos años, China podrá incrementar gradualmente su presupuesto de defensa al 3 por ciento del PIB y mantenerlo en este nivel apropiado. Eventualmente China deberá introducir su versión de la Doctrina Monroe en la política exterior china, para empujar la esfera de control o esfera de influencia estadounidense muy lejos de la periferia de China.

## Conclusión

Tanto Estados Unidos como Australia entienden muy claramente que la Batalla AireMar por sí misma no es una estrategia ganadora. Derrotar a China mediante la guerra depende principalmente del quebrantamiento económico y psicológico dentro de China. Así como Estados Unidos cree que interrumpiendo las líneas marítimas de comunicación de China desacelerará su economía, lo que a su vez creará desorden interno, China cree que debe reducir su dependencia en el comercio exterior a la vez que impulsa la demanda y oferta interna. En esencia, la estabilidad económica y política interna será crucial para vencer cualquier bloqueo o intervención militar percibido o planeado. □

### Notas

1. John Pomfret, “Beijing Claims ‘Indisputable Sovereignty’ over South China Sea (Beijing proclama ‘soberanía indisputable’ sobre el Mar del Sur de China)”, *Washington Post*, 31 de julio de 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/30/AR2010073005664.html>.

2. 陶社兰, “陈炳德: 中国能处理南海问题 美国不必操心,” 中国新闻网, 11 de julio de 2011, <http://www.chinanews.com/gn/2011/07-11/3173918.shtml>.

3. Andrew F. Krepinevich, *Why AirSea Battle? (¿Por qué la Batalla AireMar?)* (Washington, DC: Centro para Evaluaciones Estratégicas y Presupuestarias, 2010), 2, <http://www.csbaonline.org/wp-content/uploads/2010/02/2010.02.19-Why-AirSea-Battle.pdf>.

4. Hillary Rodham Clinton, Secretaria de Estado de los Estados Unidos (presentación, Centro Nacional de Convenciones, Hanoi, Vietnam, 23 de julio de 2010), <http://www.state.gov/secretary/rm/2010/07/145095.htm>.

5. Consulte, por ejemplo, Jan van Tol con Mark Gunzinger, Andrew Krepinevich, y Jim Thomas, *AirSea Battle: A Point-of-Departure Operational Concept (Batalla AireMar: Un Concepto Operativo de Punto de Partida)* (Washington, DC: Centro para Evaluaciones Estratégicas y Presupuestarias, 2010), 16, 37, <http://www.csbaonline.org/wp-content/uploads/2010/05/2010.05.18-AirSea-Battle.pdf>.

6. Ross Babbage, *Australia’s Strategic Edge in 2030 (Ventaja estratégica de Australia en 2030)*, documento Kokoda N° 15 (Kingston, Australia: Kokoda Foundation, febrero de 2011), vi, <http://www.kokodafoundation.org/Resources/Documents/KP15StrategicEdge.pdf>.

7. Secretario de Defensa Robert M. Gates (comentarios, Centro de Convenciones Gaylord, National Harbor, MD, 3 de mayo de 2010), <http://www.defense.gov/speeches/speech.aspx?speechid=1460>.

8. Nicole Gaouette, “Gates Says U.S. to Increase Asia Military Presence, Australia Defense Ties (Gates dice que EE. UU. aumentará la presencia militar en Asia, vínculos de defensa con Australia)”, *Bloomberg*, 7 de noviembre de 2010, <http://www.bloomberg.com/news/2010-11-08/gates-says-u-s-to-increase-asia-military-presence-australia-defense-ties.html>.

9. Laura Meckler, “Obama, on Australia Visit, Says U.S. Will Expand Its Presence in Region (Obama, en visita a Australia, dice que EE.UU. ampliará su presencia en la región)”, *Wall Street Journal*, 17 de noviembre de 2011, <http://online.wsj.com/article/SB10001424052970204190504577041052487222124.html>.

10. “Bush Hails ‘Sheriff’ Australia (Bush saluda a Australia como su ‘Sheriff’), *BBC News*, 16 de octubre de 2003, <http://news.bbc.co.uk/2/hi/3196524.stm>.

11. Hon. Stephen Smith, ministro australiano de defensa, “The Coming Asia-Pacific Century: What It Means for the Australia-U.S. Alliance (El próximo siglo de Asia-Pacífico: Lo que significa para la alianza entre Australia y EE.UU.)” (comentarios, Brookings Institution, Washington, DC, 27 de julio de 2011), 15, [http://www.brookings.edu/~media/Files/events/2011/0727\\_asia\\_pacific/20110727\\_australia.pdf](http://www.brookings.edu/~media/Files/events/2011/0727_asia_pacific/20110727_australia.pdf).

12. Departamento de Defensa, *Defending Australia in the Asia Pacific Century: Force 2030 (Defensa de Australia en el Siglo de Asia Pacífico: Fuerza 2030)* (Commonwealth of Australia: Departamento de Defensa, 2009), [http://apo.org.au/sites/default/files/defence\\_white\\_paper\\_2009.pdf](http://apo.org.au/sites/default/files/defence_white_paper_2009.pdf).

13. Daniel Flitton, "Rudd the Butt of WikiLeaks Exposé (Rudd el blanco de la exposición de WikiLeaks)", *Sydney Morning Herald*, 6 de diciembre de 2010, <http://www.smh.com.au/technology/security/rudd-the-butt-of-wikileaks-expos-20101205-18lf2.html>.
14. Sam Bateman y Anthony Bergin, *Sea Change: Advancing Australia's Ocean Interests (Cambio radical: Avance de los intereses oceánicos de Australia)* (Barton: Australian Strategic Policy Institute, marzo de 2009), 11, [http://www.aspi.org.au/htmlver/ASPI\\_Seachange/\\_lib/pdf/ASPI\\_Seachange.pdf](http://www.aspi.org.au/htmlver/ASPI_Seachange/_lib/pdf/ASPI_Seachange.pdf).
15. Fergus Hanson, *Australia and the World: Public Opinion and Foreign Policy (Australia y el mundo: Opinión pública y política exterior)* (Sydney: Instituto Lowy para Política Internacional, 2011), 11, <http://www.lowyinstitute.org/Publication.asp?pid=1617>.
16. Van Tol y otros, *AirSea Battle (Batalla AireMar)*, xi.
17. Departamento de Defensa, *Defending Australia (Defensa de Australia)*, 12.
18. *Ibíd.*, 137.
19. SIPRI, *SIPRI Yearbook 2011: Armaments, Disarmament and International Security (Anuario de 2011 de SIPRI: Armamentos, desarme y seguridad internacional)* (Estocolmo: Instituto de Estocolmo para la Investigación de la Paz Internacional, 2011), 183.
20. Babbage, *Australia's Strategic Edge (Ventaja estratégica de Australia)*, 51-52.
21. Departamento de Defensa, *Defending Australia (Defensa de Australia)*, 34.
22. Comunicado conjunto, Consultas Ministeriales Australia-Estados Unidos 2010, Melbourne, 8 de noviembre de 2010, <http://www.foreignminister.gov.au/releases/2010/AUSMIN-Joint-Communique.pdf>.
23. Andrew Probyn y Nick Butterly, "Nation's Military Moved West in Defence Plan (Los militares de la nación se desplazan al oeste en el plan de defensa)", *West Australian*, 22 de junio de 2011, <http://au.news.yahoo.com/thewest/a/-/newshome/9684935/nations-military-moved-west-in-defence-plan>.
24. Smith, "The Coming Asia-Pacific Century (El próximo siglo de Asia-Pacífico)," 30, 31.
25. Departamento de Defensa, *Defending Australia (Defensa de Australia)*, 47.
26. Hanson, *Australia and the World (Australia y el mundo)*, 10.
27. "US Bases in Australia (Bases estadounidenses en Australia)", Australian Anti-Bases Campaign Coalition, consultado el 18 de julio de 2011, [http://anti-bases.org/campaigns/NMD\\_PineGap/Map\\_of\\_US\\_Military\\_Bases\\_in\\_Australia.html](http://anti-bases.org/campaigns/NMD_PineGap/Map_of_US_Military_Bases_in_Australia.html).
28. Van Tol y otros, *AirSea Battle (Batalla AireMar)*, 51-52.
29. "Pakistan Demands US Vacate Air Base after Deadly Strikes (Paquistán exige que Estados Unidos desocupe base aérea después de ataques mortales)", *msnbc.com*, 27 de noviembre de 2011, [http://www.msnbc.msn.com/id/45442885/ns/world\\_news-south\\_and\\_central\\_asia/t/pakistan-demands-us-vacate-air-base-after-deadly-strikes/](http://www.msnbc.msn.com/id/45442885/ns/world_news-south_and_central_asia/t/pakistan-demands-us-vacate-air-base-after-deadly-strikes/).
30. Smith, "The Coming Asia-Pacific Century (El próximo siglo de Asia-Pacífico)," 27.



**El señor Liao Kai** (BA, Universidad de Malmo, Suecia; MSc, Universidad de Lund, Suecia) es un investigador del Instituto Knowfar para Estudios Estratégicos y de Defensa, en China. Participa en el proyecto Batalla AireMar, concentrándose en las políticas de relaciones exteriores y de defensa de Australia y su cooperación militar con Estados Unidos en el Pacífico Occidental. Anteriormente trabajó como editor de la carta de noticias *PLA and China* y como asociado de proyecto en el Instituto de Seguridad y Política de Desarrollo, en Suecia.

# El Dragón y la Computadora

## Por qué el Robo de la Propiedad Intelectual es Compatible con la Doctrina China de la Guerra Cibernética

Paulo Shakarian

Jana Shakarian

Andrew Ruef

Un fragmento del próximo libro *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Introducción a la guerra cibernética: Un enfoque multidisciplinario), publicado por Syngress (ISBN: 978-0124078147), disponible a inicios de junio del 2013. Una versión completa del capítulo se puede comprar en línea en <http://store.elsevier.com/> a inicios de mayo del 2013.

**D**URANTE LOS últimos cinco años, los medios de comunicación parecen haber estado cubiertos de presuntos incidentes cibernéticos chinos. Estas actividades han incluido casos de robo de datos científicos protegidos,<sup>1</sup> monitoreo de las comunicaciones del Dalai Lama<sup>2</sup> y el robo de propiedad intelectual de *Google*.<sup>3</sup> En un testimonio ante el Comité de Servicios Armados del Congreso, el General Keith Alexander, comandante del Comando Cibernético de Estados Unidos y jefe de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), declaró que China le está robando a Estados Unidos una “gran cantidad” de propiedad intelectual relacionada con la milicia.<sup>4</sup> Evidentemente, el espionaje cibernético, que incluye el robo de propiedad intelectual, ya es un componente clave de la estrategia cibernética china. El informe recién publicado de la empresa de seguridad *Mandiant* ofrece un análisis técnico que nos lleva a la conclusión de que una organización dentro del Ejército Popular de Liberación de China (Unidad 61398) ha sido responsable de una gran cantidad de espionaje cibernético contra países de habla inglesa.<sup>5</sup> En este artículo, destacamos algo de la doctrina china relevante que creemos condujo a la creación de organizaciones tales como la Unidad 61398 y otras.

Las actividades de extracción, monitoreo y robo de información digital descritas aquí se pueden catalogar fácilmente como incidentes de espionaje cibernético. La meta aparente de este tipo de operación cibernética no es ni desconectar las computadoras ni destruir los datos que contienen sino capturar los datos de la fuerza opositora. Siendo este el caso, dichas actividades no pueden catalogarse como ataques cibernéticos porque los sistemas que se atacan y sus datos tienen que permanecer intactos para poder obtener los datos deseados. Por ende, podemos definir el espionaje cibernético como el acto de obtener acceso a datos de un sistema de computadoras sin la autorización del dueño de ese sistema para fines de recopilación de inteligencia.

Sin embargo, al igual que los incidentes de ataque a las redes de computadoras, estos incidentes de espionaje cibernético también son claramente difíciles de atribuir. Entonces, ¿qué nos conduce a creer la participación de los chinos en los incidentes de espionaje cibernético? Si la atribución es tan difícil, ¿entonces por qué estas acciones provocan que corporaciones como *Google* y *Northrop Grumman*, al igual que diplomáticos de alto nivel como la Secretaria de Estado Hilary Clinton, hagan declaraciones severas contra el gobierno chino a raíz de esos ataques? El problema radica en el origen de los incidentes.<sup>6</sup> A menudo las computadoras involucradas con el robo de información digital se rastrean a redes que están ubicadas en China continental. Además, el análisis forense del *malware* de esos incidentes a menudo indica el uso de herramientas

para crear *software* en el idioma chino. Aunque es prácticamente imposible implicar al gobierno de la República Popular China (RPC) en estas acciones de espionaje cibernético, el hecho de que consistentemente se pueden rastrear a China continental plantea graves preguntas de política. ¿Está el gobierno chino llevando a cabo investigaciones activas contra los *hackers* (piratas cibernéticos), y qué acciones legales están tomando una vez que se identifican estos *hackers*? ¿Está el gobierno chino compartiendo claramente la información de estas supuestas investigaciones con las víctimas del espionaje cibernético? ¿Qué medidas legales está tomando Beijing para evitar que los *hackers* individuales ataque organizaciones fuera de China? Estas preguntas deben ser consideradas seriamente a raíz de los intentos de espionaje cibernético y cuando hay pruebas de orígenes chinos.

¿Qué ganaría China al ofrecer un entorno tolerante para los *hackers*? Es poco probable que el gobierno chino—que se distingue por el monitoreo de estado<sup>7</sup>—no tuviese los recursos para disminuir esa actividad. Además, se puede esperar que la reprobación generada por la comunidad internacional sea indeseable diplomáticamente. Estas actividades le proveen a la RPC beneficios importantes. La naturaleza de la información robada—que va desde detalles sobre armamento norteamericano y secretos comerciales hasta las comunicaciones del Dalai Lama—son todas de un interés particularmente elevado para Beijing. Además, a fines de la década de los noventa e inicios de la del dos mil varios pensadores militares chinos escribieron acerca del tema de la guerra cibernética.<sup>8</sup> Esos escritos indican que obtener un acceso no autorizado a los sistemas de computadoras con el propósito de extraer información es parte fundamental de la estrategia cibernética china.

Para poder comprender la doctrina china, debemos tomar en cuenta cómo las tradiciones y la cultura de esa nación han moldeado su razonamiento militar en maneras muy diferentes a las de Occidente. En un artículo *SANS*<sup>9</sup>, el Cnel Edward Sobiesk destaca un ejemplo que ilustra las diferencias amplias entre la forma de pensar Occidental y la china que se destacan en un Informe al Congreso en el 2002 titulado *The Military Power of the PRC* (El poder militar de la RPC) por el Secretario de Defensa de EE.UU.<sup>10</sup> En este informe se identifica que uno de los objetivos estratégicos de China es cómo maximizar la “configuración estratégica de poder” conocida como “shi”. En el informe, un pie de página para ‘shi’, reza como sigue: “No hay un equivalente occidental para el concepto ‘shi’. Los lingüistas chinos lo explican como ‘la alineación de las fuerzas’, la ‘inclinación de las cosas’ o ‘potencial que nace de la disposición’ de lo que solamente un estratega experto se puede aprovechar para garantizar la victoria sobre una fuerza superior”. Otra interpretación del “shi” se podría enfocar en establecer condiciones favorables. Si una nación estado logra alcanzar un nivel de “shi” más elevado que un rival, este último será derrotado fácilmente cuando el conflicto surja, porque cualquier batalla (inclusive de ser necesaria) se llevará a cabo en condiciones sumamente favorables para la primera nación—ya que ésta ha establecido las condiciones favorables mediante el logro del “shi”. Al lograr un nivel de acceso elevado a los sistemas de computadoras activos de un adversario—la información almacenada en esos sistemas ha perdido dos aspectos críticos—confidencialidad e integridad.<sup>11</sup> La *confidencialidad* garantiza que ningún individuo no autorizado pueda ver la información mientras que la *integridad* garantiza que la información, una vez extraída, no sea alterada. Eliminar estos aspectos de la información de un adversario puede contribuir en gran medida a establecer las condiciones en el campo de batalla—quizás inclusive evitar la batalla del todo. En vista de que el espionaje cibernético “shi” parece ser una herramienta estratégica formidable—al lograr acceso a los sistemas de computadora del opositor, la ventaja de la información del rival es disminuida a la vez que se logra lo mismo en el lado que la inicia.

### *De defensa activa a ofensiva activa*

Tradicionalmente, el Ejército Popular de Liberación (EPL) estaba enfocado en la idea china tradicional de “defensa activa” que se refiere a la idea de no iniciar un conflicto pero estar preparado para responder a una agresión.<sup>12</sup> En un artículo del 2008 en la revista *Military Review*, Timothy Thomas destaca que a fines de la década de los noventa e inicios de la del 2000 se produjo un cambio de esta mentalidad, particularmente con respecto a la guerra cibernética. Este paradigma que parecía surgir en ese entonces era una “ofensiva activa”. Bajo esta rúbrica nueva, la idea de establecer las condiciones del campo de batalla (o sea, desarrollar el “shi”) es aún preeminente pero la manera en que se trata de lograr dio un giro diferente. En el campo de la cibernética esto incluye no solamente fortalecer las defensas de uno para disuadir el ataque, sino utilizar las operaciones cibernéticas para obtener el control en caso de un conflicto mayor.

Esta idea de “ofensiva activa” se introdujo en 1999 en el libro titulado *Information War* (Guerra informática) por Zhu Wenguan y Chen Taiyi. En este libro, ellos incluyen una sección titulada “*Conducting Camouflaged Attacks*” (Llevando a cabo ataques camuflajeados) en los que la anticipación y la ofensiva activa se plantean.<sup>13</sup> Un componente clave de la ofensiva activa es la vigilancia de la red que incluye obtener un entendimiento del mando y control (C2, por sus siglas en inglés), guerra electrónica (EW, por sus siglas en inglés) y sistemas de armamento importantes del opositor. En el 2002 y el 2003, el General Dai Qingmin repitió algunas de esas ideas.<sup>14</sup> Él recalcó que es necesario que la información y las operaciones cibernéticas sean “precursoras” (o sea, que se lleven a cabo antes que sucedan las operaciones) y “a largo plazo” (que se lleven a cabo durante la operación). ¿Dónde encaja el espionaje cibernético en este esquema? Por ejemplo, los *hackers* rusos se aprovecharon de los ataques cibernéticos de negación de servicios en las fases iniciales de la campaña de Georgia para obstaculizar el gobierno, la banca y los sitios web de los medios de comunicación de la fuerza opositora. O sea, la anticipación también puede adoptar otras formas más sutiles. Por ejemplo, tener acceso constante a los sistemas de informática tibetanos verdaderamente sería una ventaja y probablemente resultaría en la posibilidad de evitar completamente un conflicto abierto. El robo de secretos militares relacionados con sistemas de armamento nuevos le podría dar a los chinos la inteligencia técnica (TECHINT, por sus siglas en inglés) necesaria para encontrar vulnerabilidades o inclusive diseñar sus propias copias de dicho armamento. Robar propiedad intelectual de los vendedores de *software* le podría dar a los *hackers* chinos un caudal de conocimientos necesarios para identificar vulnerabilidades nuevas para futuros ataques cibernéticos y operaciones de espionaje cibernético.

La obra *Information War* y los escritos del General Dai ilustran la importancia del aspecto cibernético a las operaciones militares chinas. No obstante, muchos de los incidentes de espionaje cibernético que trataremos en este artículo tienen que ver con el robo de información de empresas privadas durante tiempos de paz. ¿Cómo se explica esto en la literatura china sobre la guerra cibernética? Las respuestas a preguntas de este tipo parecen radicar en el libro de 1999 titulado *Unrestricted Warfare* (Guerra irrestringida) por los Coroneles Qiao Liang y Wang Xiangsui del EPL.<sup>15</sup> En esta obra, los autores afirman que la guerra moderna se extiende más allá de un simple ámbito militar. La guerra moderna incluye líderes políticos, científicos y económicos además del personal militar. La noción de una guerra “irrestringida” extiende no solo los ámbitos de la guerra sino también el tiempo en que esas acciones de guerra pueden ocurrir. Las operaciones “militares”—que ahora incluyen aspectos de información, económicos y psicológicos, pueden tener lugar durante tiempos de paz en esta perspectiva—apoyando aún más la noción de “ofensiva activa”. Esto puede que ayude a explicar por qué el inicio del siglo XXI ha estado cubierto con relatos de espionaje cibernético chino contra corporaciones y laboratorios científicos.

En ese mismo orden de ideas, el Coronel Wang Wei y el Mayor Yang Zhen del Departamento de Guerra y Comando de Informática de la Academia Militar Nanjing escribieron en *China Military Science* que en una guerra contra una sociedad centrada en la informática, el sistema político,

el potencial económico y los objetivos estratégicos de una nación serán blancos de gran valor.<sup>16</sup> Luego pasan a describir que el método preferido para atacar dicha sociedad sería a través del uso de técnicas de guerra asimétrica. Guerra asimétrica se refiere a la capacidad de un combatiente de derrotar una fuerza superior empleando tácticas que le sacan provecho a las debilidades más importantes en sus sistemas de armamento, tácticas o tecnología de informática. Durante la guerra de Estados Unidos en Iraq del 2003 al 2011, los insurgentes a menudo empleaban ataques asimétricos tales como bombas en las carreteras a diferencia de ataques más tradicionales que de lo contrario los hubiesen expuesto a la potencia de fuego superior de los estadounidenses. El Coronel Wei y el Mayor Zhen apoyan los ataques asimétricos en un nivel más estratégico—específicamente haciendo un llamado a operaciones en tiempo de paz que tienen metas militares y económicas. Para lograr esas metas, bajo “condiciones informatizadas” ellos alegan que se debe llevar a cabo una guerra económica y comercial.<sup>17</sup> Evidentemente, estos autores fueron influenciados por sus ideas anteriores de *Unrestricted Warfare*. Parece que las operaciones de espionaje cibernético en tiempo de paz lanzados desde China continental contra blancos científicos, militares y comerciales son compatibles con esta línea de razonamiento.

Otra línea de razonamiento en los escritos chinos para justificar sus aparentes acciones audaces en el ciberespacio es que ellos creen que esas actividades se pueden llevar a cabo con relativa impunidad. En un artículo del 2009 en *China Military Science*, el Coronel Superior Long Fangcheng y el Coronel Superior Li Decai expresan que las operaciones cibernéticas dirigidas contra blancos sociales, económicos y políticos se pueden llevar a cabo sin temor a que esas actividades conduzcan a enfrentamientos militares a gran escala.<sup>18</sup> En ese caso, ellos por lo general consideran la guerra cibernética como un elemento de poder de persuasión—no obstante con grandes efectos. Luego pasan a alegar que el efecto final de esta forma de poder de persuasión sumamente eficaz es que la línea entre tiempo de paz y tiempo de guerra se vuelve borrosa. Esta confusión puede que sea un sello de las operaciones cibernéticas en general y podría conducir a la guerra metafórica sin final en el futuro cercano.

### ***INEW y la cibernética en el EPL***

La estrategia general de guerra de información (IW, por sus siglas en inglés) que el EPL emplea se conoce como Guerra electrónica integrada en la red (INEW, por sus siglas en inglés).<sup>19</sup> Esta estrategia originalmente se esbozó en un libro escrito en 1999 por el General Dai Qingmin titulado *On Information Warfare* (Sobre la guerra informática). Esta integración de las operaciones cibernéticas a los recursos tradicionales de la guerra de la informática es un elemento clave de la estrategia INEW. La INEW depende de la aplicación simultánea de la guerra electrónica y de las operaciones cibernéticas para abrumar el mando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR, por sus siglas en inglés) del adversario. Por ende, la misión de las piezas clave de la guerra cibernética (ataque cibernético, espionaje cibernético y defensa cibernética) son elementos asignados del Estado Mayor del EPL a los cuales tradicionalmente se le otorgan roles similares en la guerra electrónica.

El Estado Mayor del EPL está dividido en varios departamentos. INEW por lo regular asigna tareas ofensivas (ataque cibernético y contramedidas electrónicas [ECM, por sus siglas en inglés] más convencionales) al 4º Departamento—que tradicionalmente ha desempeñado un papel más importante en la guerra de informática ofensiva.<sup>20</sup> Cabe destacar que el General Dai Qingmin fue ascendido a jefe del 4º Departamento en el 2000—quizás un indicio de que el EPL tenía intenciones de adoptar su visión de INEW. Las tareas de defensiva e inteligencia—específicamente defensa cibernética y espionaje cibernético—están asignadas al 3º Departamento—que tradicionalmente se enfocaba en la inteligencia de señales (SIGINT, por sus siglas en inglés).<sup>21</sup> Se piensa que el 3º Departamento es la sede de las Agencias de Reconocimiento Técnico cuya misión normal es la recopilación de SIGINT. A fines de la década de los años noventa, varias de estas

agencias recibieron reconocimientos relacionados con investigaciones en la guerra informática.<sup>22</sup> Algunos analistas creen que esto es señal del papel que desempeñan en las operaciones cibernéticas.<sup>23</sup>

Para fortalecer a los especialistas de guerra informática en el 3<sup>er</sup> y el 4<sup>o</sup> GSD, los chinos también han establecido unidades de milicia de guerra informática.<sup>24</sup> Esas milicias pueden considerarse como una “guardia nacional cibernética” ya que constan en su mayoría de personal de la tecnología de informática comercial (IT, por sus siglas en inglés) y de entornos académicos. Informes de fuentes abiertas indican que estas unidades fueron creadas desde el 2003 al 2008 en las provincias de Guangzhou, Tianjin, Henan y Ningxia.<sup>25</sup> Inclusive hay pruebas de que algunas de esas milicias recibieron tareas en tiempo de guerra específicas—la mayoría de las cuales parecen estar enfocadas en el ataque cibernético.<sup>26</sup>

Las ideas principales de las operaciones cibernéticas chinas surgieron de los escritos de oficiales del ELP a fines de la década de los noventa y finalmente implementadas en la estrategia INEW que coinciden con las responsabilidades de ataque cibernético y de espionaje cibernético con organizaciones que llevan a cabo operaciones similares en el ámbito de la guerra electrónica.<sup>27</sup> Aunque la comunidad de *hackers* chinos saltó a la fama a fines de los años noventa e inicios del 2000 con ataques que aparentemente tenían metas congruentes con el gobierno, el ELP en un final desaprobó esas acciones.<sup>28</sup> Como resultado, muchos de los “*hackers*” se han convertido en “sombbrero blanco” ya sea transformando sus grupos de *hackers* en empresas asesoras u obteniendo empleo con el gobierno o el ámbito académico.<sup>29</sup> El ámbito académico chino también parece estar sumamente involucrado con la guerra cibernética—no tan solo en las investigaciones sino también posiblemente con las operaciones.<sup>30</sup>

### ***Estudio de un caso práctico sobre la guerra cibernética mediante el robo de propiedad intelectual: Operación Aurora***

El 20 de enero de 2010, *Google* anunció una noticia impactante. La empresa publicó en su *blog* oficial que había sido víctima de una guerra cibernética originando de China. Según el *blog*, la finalidad de la operación fue lograr acceso a las cuentas de correo electrónico *Gmail* de los activistas chinos de derechos humanos.<sup>31</sup> Como resultado de esta operación de espionaje cibernético, *Google* anunció que ya no censuraría los resultados en su buscador principal en China—*google.cn*—una medida que causó consternación con la RPC. La empresa expresó que si no podía funcionar su buscador sin censura, estaría dispuesta a cerrar operaciones en China.

Literalmente minutos después del anuncio de *Google*, *Adobe*—otro vendedor importante de *software*—anunció que sus sistemas corporativos también habían sido víctimas de los *hackers*.<sup>32</sup> Resulta que tanto *Google* como *Adobe* fueron blancos del mismo adversario—un adversario que llevó a cabo la misma operación contra 32 otras empresas. Entre ellas se encontraban *Dow Chemical*, *Northrop Grumman*, *Symantec* y *Yahoo*.<sup>33</sup> Parece que el propósito de la operación era extraer no tan solo información acerca de los activistas chinos de derechos humanos, sino también de la propiedad intelectual—principalmente el código fuente de *software* diseñado comercialmente.<sup>34</sup>

Esta operación—conocida como “Operación Aurora”—es el tema de esta sección. Se aprovechó de las ingenierías sociales junto con un virus *Trojan* conocido como *Hydraq* para robar propiedad intelectual. Varios analistas tienen la firme sospecha de la participación de la RPC. En esta sección analizamos el ataque y las pruebas de la participación de la RPC y discutimos las consecuencias del robo de propiedad intelectual de las corporaciones.

Este acto de espionaje cibernético empleó una vulnerabilidad en *Microsoft Internet Explorer* que fue explotada por un *software* conocido designado como *Trojan.Hydraq* por la empresa de seguridad, *Symantec*. Al igual que con varias de las operaciones de espionaje cibernético discutidas en este artículo, la Operación Aurora fue iniciada con *spear phishing* (ataques a una organización determinada). En el caso del robo en *Google*, se cree que ese *spear phishing* inicial fue dirigido a

un empleado que utilizaba el *software* de *chat* instantáneo, *Microsoft Messenger*. Supuestamente el usuario recibió un enlace a un sitio web malicioso durante uno de sus *chats*.<sup>35</sup> Se desconoce si las operaciones contra las otras empresas también fueron iniciadas con *software* de *chat*. Con base en operaciones similares parece posible que el correo electrónico puede que se halla usado como una manera para iniciar la infiltración del *software* malicioso. En cualquier caso, la comunicación inicial a estas empresas tenía tres características. Primero, fueron enviadas a un grupo selecto de individuos, lo que sugiere que este tipo de ataque (*spear phishing*) indica que los *hackers* contaban con alguna fuente de inteligencia adicional con respecto a sus blancos. Segundo, las comunicaciones fueron diseñadas de manera que parecían haber originado de una fuente confiable, lo que también muestra que los infractores estaban operando con perfiles de sus blancos. Tercero, todos contenían un enlace a un sitio web—al hacer clic iniciaba una serie de eventos.

Una vez que el usuario hacía clic en el enlace, el buscador visitaba un sitio en Taiwán. Este sitio web, a su vez, ejecutaba un código *JavaScript* malicioso—este es el código fuente que opera en un sitio web que generalmente se utiliza para proveerle al usuario características interactivas. El código *JavaScript* malicioso se aprovechó de una debilidad en el buscador *Microsoft Internet Explorer* que en aquel entonces se desconocía. A menudo una vulnerabilidad nueva de esa índole se le llama una “intrusión de día cero”. El malévolo código *JavaScript* procede a descargar un segundo pedazo de *malware* de Taiwán—disfrazado de un archivo de imagen. Este segundo *software* malicioso pasaría a funcionar en *Windows* y establecería una puerta trasera permitiéndole al espía cibernético acceso al sistema que se va a atacar.<sup>36</sup> Una puerta trasera se refiere a un método de lograr acceso a un sistema que le permite al intruso a circunvalar el mecanismo de seguridad normal. El uso de una intrusión de día cero es importante porque identificar una vulnerabilidad de ese tipo probablemente requeriría un esfuerzo de ingeniería hábil. Esto, junto con la campaña de *spear phishing* sumamente precisa (sugiriendo que los *hackers* tenían acceso a información de inteligencia adicional sobre sus blancos), podría dar a entender el apoyo de una organización más grande—quizás una nación estado.

### ***Robo de propiedad intelectual***

Varios meses después que *Google* anunció que había sido atacada, el *New York Times* informó que se habían comprometido mucho más que tan solo cuentas de correo electrónico de activistas chinos de derechos humanos. Nombrando una fuente no identificada con conocimiento directo sobre la investigación de *Google*, el periodista John Markoff escribió que el código fuente al sistema moderno de contraseñas de *Google* probablemente había sido robado durante la Operación Aurora.<sup>37</sup> El sistema, conocido como *Gaia*, fue concebido para permitirles a los usuarios del *software* de *Google* utilizar un solo nombre de usuario y contraseña para tener acceso a una variedad de servicios de *Google*. Este *software* también se conoce como “*Single Sign-On*”. Markoff informó que *Google* enfrentó el problema añadiendo una capa adicional de codificación a su sistema de contraseña.

La puesta en peligro de *Gaia* es importante por más de un motivo. Primero, obtener el código fuente del *software* de un sistema comercial es robo de la propiedad intelectual y por ende ilegal en Estados Unidos. Al igual que con los datos robados durante *Titan Rain*, el código fuente le permitiría a ciertos diseñadores crear *software* ilícito similar a *Gaia*. Si consideramos la Operación Aurora como las acciones de una nación estado, se podría pensar que el robo de propiedad intelectual es una forma de guerra económica—nivelar el campo de juego tecnológico para reducir la ventaja de la capacidad industrial de una nación adversaria. Evidentemente, esto está en línea con las ideas chinas de *Unrestricted Warfare*—donde varias formas de guerra informática ocurren constantemente (inclusive durante tiempos de paz) y atacan todos los aspectos del poder de una nación (incluyendo la industria).

Sin embargo, más allá de las ventajas económicas obtenidas por el robo de códigos fuentes, implicaciones importantes de seguridad también son inminentes—en particular en el caso de *Gaia*. Por ejemplo, los analistas que trabajan con los *hackers* probablemente determinarían las vulnerabilidades técnicas en el sistema de contraseñas.

Si bien está claro que el robo de propiedad intelectual es una consideración importante para las corporaciones, también plantea una pregunta importante. ¿Cómo pudieron los *hackers* obtener el código fuente para un sistema como *Gaia* al hacer uso de una cifra relativamente pequeña de sistemas de computadoras comprometidos? Resulta que muchas corporaciones trabajan con servidores especializados como almacenes para este tipo de datos—a menudo correctamente referidos como “depósitos de propiedad intelectual”. Las ubicaciones centralizadas de este tipo de datos facilitan que los equipos trabajen en colaboración en un proyecto y compartan información entre ellos. Estos sistemas a menudo toman la forma de sistemas de Gestión de Configuración de *Software* (SCM, por sus siglas en inglés) tales como *IBM Rational*<sup>®</sup> o sistemas de gestión de contenido tales como *Microsoft SharePoint*<sup>®</sup>.

La Operación Aurora invalidó una suposición importante hecha por muchos administradores de sistemas y vendedores de almacenes IP de *software* en ese momento. Los profesionales que operan esas redes dan por sentado que no habría acceso a la propiedad intelectual a causa de las contramedidas de seguridad adoptadas para proteger a la red en general. El resultado de esta perspectiva y menos enfoque en la seguridad de un depósito IP que se encuentra dentro del perímetro de la red de una corporación. Al utilizar una vulnerabilidad de día cero para su misión, los infractores detrás de la Operación Aurora pudieron aprovecharse de esa suposición.

El robo de la propiedad intelectual presenta otra dificultad importante—determinar qué se robó en realidad. A raíz de la Operación Aurora, el investigador de seguridad, George Kurtz, escribió un artículo titulado “*Where’s the body?*” (¿Dónde está el cadáver?).<sup>38</sup> A diferencia de un robo físico donde es relativamente fácil definir qué fue lo que se robó, con el espionaje cibernético y la extracción de datos eso es mucho más difícil de establecer. Aunque los administradores de sistemas tienen a la mano unas cuantas herramientas—tales como el análisis de registros de servidores y del tráfico en la red—en las operaciones avanzadas de espionaje cibernético los *hackers* a menudo toman varias medidas para encubrir sus pasos y operar en una manera que dificulta determinar cuáles datos fueron robados. Aunque los vendedores de seguridad proveen soluciones de *software* para ayudar con este problema, determinar “¿dónde está el cadáver?” a raíz de una operación de espionaje cibernético aún es una tarea difícil.

### ***Indicadores de la participación de la RPC***

Resulta interesante que el anuncio de *Google* sobre la violación de seguridad parece implicar la participación de los chinos—o al menos sugiere descuido por parte del gobierno. A continuación se ofrecen algunos indicadores que la Operación Aurora fue ejecutada con el pleno conocimiento o inclusive bajo la dirección del gobierno chino.

Las primeras señales de la participación china se publicaron en enero de 2010—varias semanas después del mensaje de *blog* de *Google*. Un informe publicado por la empresa de seguridad *VeriSign* alegaba que los “IP fuentes” y el servidor de descarga (*drop server*) repositorio del ataque corresponden a una sola entidad extranjera que consta o bien de agentes del estado chino o *proxys* del mismo”.<sup>39</sup> Los investigadores en *VeriSign* también descubrieron que los *hackers* Aurora utilizaron *HomeLinux DynamicDNS* y tomaron prestadas direcciones IP de la empresa norteamericana *Linode* (una compañía que se especializa en el alojamiento de servidores privados virtuales). Estas son las mismas circunstancias de los ataques DDoS en julio de 2009 contra Corea del Sur y Washington, D.C. Cuando se consideraron con otras circunstancias similares, los investigadores de *VeriSign* concluyeron que Aurora y los ataques contra Washington, D.C., y Corea del Sur posiblemente los llevó a cabo la misma entidad.

Pocas semanas después, periodistas del *New York Times*. John Markoff y David Barboza, publicaron un artículo que alegaba que los investigadores habían identificado que dos escuelas chinas de estudios superiores habían participado en el ataque—*Shanghai Jiaotong University* y *Lanxiang Vocational School*.<sup>40</sup> El *Security Engineering Institute* de ésta es el lugar de trabajo de Peng Yinan (supuestamente el hacker chino “CoolSwallow”). Cuando los periodistas del *New York Times* llevaron a cabo una entrevista telefónica anónima con un profesor de ese instituto, se sorprendieron con la respuesta cándida. Él declaró que el *hacking* de las redes de computadoras extranjeras por parte de los estudiantes era “bastante normal”.<sup>41</sup> Sin embargo, como una explicación alternativa, el profesor declaró que la dirección IP de la Universidad también pudo haber sido pirateada y según él eso “sucedió a menudo”.<sup>42</sup> En la *Lanxiang Vocational School*, los investigadores pudieron identificar una clase específica dictada por un profesor ucraniano quien se sospechaba estaba involucrado en la Operación Aurora.<sup>43</sup> Cuando se le confrontó con la sospecha, el decano del departamento de ciencias computacionales ahí (identificado por los medios de comunicación solamente como el Sr. Shao) expresó que los estudiantes en la escuela sencillamente no tendrían la capacidad de llevar a cabo un ataque de ese tipo. No obstante, sí admitió que los estudiantes de la escuela a menudo eran reclutados en la milicia.<sup>44</sup>

Los informes sobre la participación china pudieron haber inspirado el discurso de la Secretaria de Estado estadounidense, Hillary Clinton, sobre libertad en la *Internet* pronunciado poco después del anuncio de *Google*.<sup>45</sup> En este discurso ella hizo un llamado a China para que llevara a cabo una investigación transparente sobre las violaciones de *Google*. Este fue quizás la declaración más contundente hecha por un funcionario de alto rango del gobierno estadounidense planteado en respuesta al incidente de guerra cibernética en ese momento.

La Operación Aurora ilustra la evolución continua del espionaje cibernético a inicios del siglo XXI. En este caso de espionaje cibernético, la información específica fue considerada tan importante que los operadores utilizaron una explotación de día cero y *spear phishing* para lograr el acceso a los sistemas corporativos, localizar los depósitos de propiedad intelectual del blanco y robar secretos de la compañía. Reportada originalmente por *Google*, esta operación afectó a más de treinta empresas de renombre. La información robada probablemente solo fue para promover ganancias económicas, pero también es posiblemente beneficiosa para la inteligencia técnica, tales como la evaluación de vulnerabilidades—posiblemente para utilizarla en ataques cibernéticos adicionales. La Operación Aurora anuló las suposiciones existentes acerca de los depósitos de propiedad intelectual en las corporaciones y destacó una vez más la dificultad de determinar los pormenores de los datos capturados. Los informes de los medios de comunicación de la posible participación de China resultaron en una declaración diplomática por parte de la Secretaria de Estado de EE.UU. La Operación Aurora no es única. En su secuela, ha habido otras maniobras cibernéticas atribuidas a China con la meta de robar propiedad intelectual. Una serie de eventos conocidos como *Nitro*<sup>46</sup> (dirigidos en contra de la industria química) y *Night Dragon*<sup>47</sup> (contra el sector de energía) son tan solo dos ejemplos. Por último, hay muchos posibles efectos de segundo y tercer orden de un vendedor importante de *software* como *Google* o *Adobe* que ha sido pirateado. Se desconoce qué consecuencias tendría el posible conocimiento de *software* ampliamente usado, tal como el sistema de contraseña *Gaia* de *Google*, en las operaciones cibernéticas de seguimiento. Aunque en la actualidad no está conectado con Aurora, recientemente se reveló que el sistema de certificados de *software* de *Adobe* fue pirateado—permitiendo que *software* malicioso creara suplementos (*add-ons*) supuestamente seguros a muchos de los *software* de esa empresa.<sup>48</sup> En este caso, un servidor de desarrollo en *Adobe* fue asaltado. Es un ejemplo claro de cómo la seguridad cibernética de los propios sistemas de un vendedor de *software* importante puede tener un impacto directo en una población de usuarios sumamente grande—por ende ofreciéndole amplias oportunidades a un adversario que lleva a cabo ataques cibernéticos de seguimiento.

En este artículo hemos discutido varias ideas patrocinadas por pensadores militares de China sobre la guerra informática—destacando las ideas de *Unrestricted Warfare*—en las que se piensa que las operaciones cibernéticas se extienden a tiempos de paz e incluye ámbitos militares, políticos, económicos y científicos. Analizamos cómo los chinos estructuraron a sus guerreros cibernéticos en torno a la estrategia INEW. En el ELP, las operaciones cibernéticas se colocaron bajo la responsabilidad de organizaciones con misiones similares en el ámbito de la guerra electrónica. Por último, pudimos ver cómo esas ideas pueden haberse puesto en práctica con la Operación Aurora donde una explotación de día cero le permitió a los operadores robar propiedad intelectual de los depósitos en *Google*, *Adobe* y muchas otras compañías importantes a fines del 2009. □

## Notas

1. Steve DeWeese, Bryan Krekel, George Bakos, Christopher Barnett, *Capability of the People's Republic of China to Conduct of Cyber Warfare and Computer Network Exploitation* (Capacidad de la República Popular China de llevar a cabo guerra cibernética y explotación de redes de computadoras), *Northrop Grumman*, octubre de 2009.

2. *Information Warfare Monitor*, *Tracking Gh0stNet: Investigating a Cyber Espionage Network* (Rastreado a Gh0stNet: Investigando una red de espionaje cibernético), marzo de 2009.

3. Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies" (*Hackers de Google atacaron los códigos fuente de más de 30 compañías*), *Wired Threat Level*, 13 de enero de 2010, consultado el 8 de enero de 2012. Disponible en: <http://www.wired.com/threatlevel/2010/01/google-hack-attack/>.

4. J. Nicholas Hoover. (2012, marzo, 27). *NSA Chief: China behind RSA Attacks* (Jefe de NSA: China detrás de ataques RSA). *InformationWeek*. Obtenido de: [http://www.informationweek.com/news/government/security/232700341?cid=RSSfeed\\_IWK\\_All](http://www.informationweek.com/news/government/security/232700341?cid=RSSfeed_IWK_All).

5. "APT1: Exposing One of China's Cyber Espionage Units" (APT1: Exponiendo una de las unidades de espionaje cibernético de China), *Mandiant*. Obtenido de: <http://intelreport.mandiant.com/>.

6. El origen no puede referirse solamente al IP fuente mencionado (rastreado a través de *proxies* intermedios) sino también el origen del *software* determinado por el análisis técnico del código (por ejemplo, el origen basado en la versión del compilador y el lenguaje del sistema operativo empleado para crear el *software* en cuestión).

7. "Chinese Internet Giants Agree to Help Government Monitor Information" (Gigantes de *Internet* chinos acuerdan ayudar al gobierno a monitorear información), *Voice of America News*, 5 de noviembre de 2011, <http://www.voanews.com/content/chinese-internet-giants-agree-to-help-government-monitor-information-133327903/168182.html> (consultado el 25 de marzo de 2013).

8. Timothy Thomas, "China's Electronic Long-Range Reconnaissance" (Reconocimiento electrónico a gran distancia de China), *Military Review*, *Noviembre-Diciembre* 2008, 47-54.

9. Edward Sobiesk, "Redefining the Role of Information Warfare in Chinese Strategy" (Definiendo nuevamente el papel que desempeña la guerra de informática en la estrategia china), *SANS Institute InfoSec Reading Room*, marzo de 2003, [http://www.sans.org/reading\\_room/whitepapers/warfare/redefining-role-information-warfare-chinese-strategy\\_896](http://www.sans.org/reading_room/whitepapers/warfare/redefining-role-information-warfare-chinese-strategy_896) (consultado el 22 de diciembre de 2011).

10. Oficina del Secretario de Defensa de los Estados Unidos de Norteamérica, Informe al Congreso sobre el Poder Militar de la República Popular China, 12 de julio de 2002, 5-6.

11. W. V. Maconachy, Corey D. Schou, Daniel Ragsdale, Don Welch, "A Model for Information Assurance: An Integrated Approach" (Un modelo para garantía en la información: Un método integrado), *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security* (Ponencias del Taller IEEE 2001 sobre garantía y seguridad de la información), junio de 2001, <http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf> (consultado el 22 de diciembre de 2011).

12. Timothy Thomas, "China's Electronic Long-Range Reconnaissance", *Military Review*, *Noviembre-Diciembre* de 2008, 47-54.

13. *Ibíd.*

14. *Ibíd.*

15. Sobiesk, 8.

16. Timothy Thomas, "Google Confronts China's Three Warfares" (*Google enfrenta las tres guerras de China*), *Parameters*, Verano 2010, 101-105.

17. Wang Wei and Yang Zhen, "Recent Development in the Study of the Thought of People's War under Informatized Conditions" (Desarrollos recientes en el estudio de la opinión de la guerra popular bajo condiciones de informática), *China Military Science*, 2ª edición 2009.

18. Long Fangcheng y Li Decai, "On the Relationship of Military Soft Power to Comprehensive National Power and State Soft Power" (Sobre la relación del poder de persuasión militar a poder nacional exhaustivo y poder de persuasión estatal), *China Military Science*, Issue 5, 2009, 120-29.

19. Steve DeWeese, Bryan Krekel, George Bakos, Christopher Barnett, *Capability of the People's Republic of China to Conduct of Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, octubre de 2009.
20. *Ibíd.*
21. *Ibíd.*
22. *Ibíd.*
23. *Ibíd.*
24. *Ibíd.*
25. *Ibíd.*
26. *Ibíd.*
27. *Ibíd.*
28. *Ibíd.*
29. *Ibíd.*
30. *Ibíd.*
31. David Drummond, "A new approach to China" (Un nuevo acercamiento a China), *The Official Google Blog*, 12 de enero de 2010. Consultado el 8 de enero de 2012. Disponible en: <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.
32. Pooja Prasad, "Adobe Investigates Corporate Network Security Issue" (Adobe investiga problema de seguridad de la red de la corporación), *Adobe Featured Blogs*, 12 de enero de 2010. Consultado el 8 de enero de 2012. Disponible en: [http://blogs.adobe.com/conversations/2010/01/adobe\\_investigates\\_corporate\\_n.html](http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html).
33. Kelly Jackson Higgins, "More Victims Of Chinese Hacking Attacks Come Forward" (Se presentan más víctimas de ataques piratas chinos), *Dark Reading*, 14 de enero de 2010, consultado el 8 de enero de 2012. Disponible en: <http://www.darkreading.com/security/attacks-breaches/222301032/index.html>.
34. Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies", *Wired Threat Level*, 13 Jan. 2010, accessed 8 Jan. 2012. Available at: <http://www.wired.com/threatlevel/2010/01/google-hack-attack/>.
35. John Markoff, "Cyberattack on Google Said to Hit Password System" (Se dice que ataque cibernético a Google atacó sistema de contraseñas), *New York Times*, 19 de abril de 2010. Disponible en: <http://www.nytimes.com/2010/04/20/technology/20google.html>, accessed 15 Jan., 2012.
36. McAfee Labs y McAfee Foundation Professional Service, "Protecting Your Critical Assets: Lessons Learned from Operation Aurora" (Protegiendo sus recursos críticos: Lecciones aprendidas de la Operación Aurora), *McAfee White Paper*, 2010.
37. John Markoff, "Cyberattack on Google Said to Hit Password System", *New York Times*, 19 de abril de 2010. Disponible en: <http://www.nytimes.com/2010/04/20/technology/20google.html>, consultado el 15 de enero de 2012.
38. George Kurtz, "Where's the body" (¿Dónde está el cadáver?), *McAfee Blog Central*, 25 de enero de 2010. Disponible en: <http://siblog.mcafee.com/cto/where%E2%80%99s-the-body/>, consultado el 15 de enero de 2012.
39. Informe de VeriSign iDefense Security Lab citado por Ryan Paul, "Researchers identify command servers behind Google attack" (Investigadores identifican servidores del comando detrás de ataque a Google), *ArsTechnica*, enero de 2010. Disponible en: <http://arstechnica.com/security/news/2010/01/researchers-identify-command-servers-behind-google-attack>.ars, consultado el 15 de enero de 2012.
40. John Markoff and David Barboza, "Two Chinese Schools Said to be Tied to Online Attacks" (Se dice que dos escuelas chinas están ligadas a ataques en línea), *New York Times*, 19 de febrero de 2010.
41. *Ibíd.*
42. *Ibíd.*
43. Al momento de este artículo, la extensión de la participación de la clase y el nombre del profesor ucraniano no están disponibles en informe de fuente abierta.
44. *Ibíd.*
45. Hillary Rodham Clinton, "Remarks on Internet Freedom" (Comentarios sobre libertad en la Internet), 21 de enero de 2010. Disponible en: <http://www.state.gov/secretary/rm/2010/01/135519.htm>, consultado el 15 de enero de 2010.
46. Eric Chien, Gavin O'Gorman, "The Nitro Attacks, Stealing Secrets from the Chemical Industry" (Los ataques Nitro, robándole secretos a la industria química), *Symantec Security Response*, 2011.
47. "Global Energy Cyberattacks: 'Night Dragon'", *McAfee White Paper*, 10 de febrero de 2011.
48. Lucian Constantin, "Hackers Compromise Adobe Server, Use it to Digitally Sign Malicious Files" (Hackers comprometen servidor Adobe, lo emplean para firmar digitalmente archivos maliciosos), *CIO*, 27 de septiembre de 2012, disponible en: [http://www.cio.com/article/717494/Hackers\\_Compromise\\_Adobe\\_Server\\_Use\\_it\\_to\\_Digitally\\_Sign\\_Malicious\\_Files](http://www.cio.com/article/717494/Hackers_Compromise_Adobe_Server_Use_it_to_Digitally_Sign_Malicious_Files), consultado el 14 de octubre de 2012.

**Las opiniones en este artículo son las de los autores y no necesariamente reflejan las opiniones ni del Departamento de Defensa de Estados Unidos, ni del Ejército de Estados Unidos, ni de la Academia Militar de Estados Unidos.**



**El Dr. Paulo Shakarian, PhD**, cuenta con un doctorado en ciencias computacionales y es un Mayor en el Ejército de Estados Unidos. Actualmente es profesor adjunto en *West Point* donde dicta clases en ciencias computacionales y tecnología de informática. Ha escrito más de veinte artículos publicados en varias revistas científicas y militares. Anteriormente sus obras han sido publicadas en *The Economist*, *WIRED* y *Popular Science*.



**La Sra. Jana Shakarian** cuenta con una maestría en sociología y antropología y anteriormente se desempeñó en calidad de científica investigadora en el Laboratorio para Dinámica Computacional Cultural de la University of Maryland y como asesora independiente con el *Network Science Center* en *West Point*.



**El Sr. Andrew Ruef** es ingeniero ejecutivo de sistemas en la empresa *Trail of Bits* (New York, NY) donde lleva a cabo análisis de seguridad de informática. Cuenta con casi una década de experiencia en la industria de seguridad en la red de computadoras e ingeniería de *software*.

# Reenfoque del Pensamiento de la Guerra Cibernética

MAYOR SEAN C. BUTLER, USAF



**E**N SEPTIEMBRE DE 2007, más de 65 expertos en este asunto de toda la Fuerza Aérea reunida en la Academia de la Fuerza Aérea de EE.UU. se reunieron para hablar sobre la forma de institucionalizar el desarrollo del adiestramiento y de las fuerzas cibernéticas.<sup>1</sup> Esta ocasión fue la continuación del establecimiento de un Cibercomando de la Fuerza Aérea (AFCYBER) provisional (un comando importante) en Noviembre de 2006, que fue la continuación a su vez, de la incorporación del ciberespacio de la Fuerza Aérea en su declaración de su misión menos de un año antes. Los defensores del ciberpoder de la década hasta este momento pudieron finalmente alcanzar el momento de establecer el ciberespacio como un dominio de combate completamente reconocido. Desgraciadamente, estas victorias se produjeron con un costo—un hecho que empezó a hacerse evidente en el congreso de 2007.<sup>2</sup>

Los organizadores del congreso mostraron a los participantes la definición del ciberespacio adoptada por el Departamento de Defensa (DOD) en su *Estrategia militar nacional para operaciones ciberespaciales*, publicada en 2006: “Un dominio caracterizado por el uso de componentes electrónicos y el espectro electromagnético a fin de almacenar, modificar e intercambiar datos por medio de sistemas de redes e infraestructuras físicas relacionadas”.<sup>3</sup> También describían el esquema del plan de la Fuerza Aérea para estructurar el campo de carreras cibernéticas, con dos “fragmentos” cibernéticos principales para operadores de redes de computadoras y oficiales de sistemas de combate (guerra electrónica).<sup>4</sup> Casi inmediatamente después, esta revelación desembocó en algunas preguntas incómodas e implicaciones extrañas. ¿Por qué puso el servicio dos campos profesionales tan diferentes en un solo conducto de adiestramiento? ¿Pertencen las interferencias de radar a la misma clase de guerra que el pirateo de redes de computadoras? ¿Significa esto que debemos considerar la parte del láser en vuelo parte del cibercombate, ya que utiliza el espectro electromagnético? Los participantes, aviadores experimentados procedentes de ambos lados, hicieron estas y otras preguntas, que se quedaron en gran medida sin contestar.

Afortunadamente, tanto el DOD como la Fuerza Aérea han corregido o eliminado el énfasis de la mayoría de los problemas mencionados arriba que están debajo de esta estructura, pero sin un cambio sustancial. Menos de dos años después de la publicación de la definición del ciberespacio en la *Estrategia Militar Nacional para Operaciones de Ciberespaciales*, el DOD la actualizó convirtiéndola en un fundamento para la doctrina más concentrado y práctico, aunque quizás innecesariamente específico: “Dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnología de información, incluida Internet, redes de telecomunicaciones, sistemas de computadora y procesadores y controladores empotrados”.<sup>5</sup> Poco después, la Fuerza Aérea disminuyó la categoría del comando mayor de AFCYBER provisional a una fuerza aérea numerada subordinada al nuevo comando subordinado del Cibercomando de EE.UU., y no incorporó nunca completamente a oficiales de sistemas de combate en su campo profesional cibernético.<sup>6</sup> En su mayor parte, el servicio abandonó el enfoque explícito en el espectro electromagnético y las características físicas.

Los esfuerzos de los primeros defensores del ciberpoder de atraer la atención y los recursos al ciberespacio como un dominio operacional militar han dado fruto en años recientes.<sup>7</sup> No obstante, el cuerpo de la teoría y la doctrina que se desarrollaron fueron influidos indiscutiblemente (posiblemente de forma inconsciente) por el propio proceso de lucha por superar la resistencia conservadora. Los temas recurrentes tratan de describir el ciberespacio como más cómodamente análogo a los dominios tradicionales de tierra, mar, aire y espacio. Además de resaltar sus características físicas, la doctrina actual transfiere los principios y fundamentos básicos de otros dominios operacionales al ciberespacio, asumiendo aparentemente, sin una consideración cuidadosa, su aplicabilidad al nuevo contexto. (El artículo examina más adelante algunos ejemplos de esta práctica).

El ciberespacio incuestionablemente tiene un elemento físico que conlleva ciertas implicaciones de combate, y muchos principios de guerra fundamentales se aplicarán sin duda a la ciber guerra. No obstante, el método es defectuoso, porque la doctrina parece buscar formas de demostrar que el “ciberespacio es como otro dominio” en vez de tener en cuenta sus propiedades exclusivas. En vez de continuar concentrándose en los elementos físicos relativamente mundanos del ciberespacio, los pensadores militares deben abrazar su exclusiva naturaleza lógica o virtual y considerar sus implicaciones. Entender la exclusividad del ciberespacio aclara de forma básica el pensamiento hacia la ampliación de la teoría específica del dominio y de la formulación de doctrina.

## El ciberespacio como dominio físico

Los primeros intentos de describir el ciberespacio como dominio operacional tendían a hacer énfasis en que estaban basados en el mundo físico como característica definidora. Nuevamente, esto es entendible, ya que los pensadores teóricos estaban tratando de establecer el ciberespacio como un dominio a la par con la tierra, el mar, el aire y el espacio—con todos los dominios del mundo físico. Los proponentes trataron de obtener su propia sección del mismo universo físico a fin de poner el ciberespacio completamente junto con los otros dominios tradicionales.

En su trabajo original *Guerra estratégica en el ciberespacio*, uno de los primeros estudios más influyentes de la ciberguerra, el Coronel Gregory Rattray, USAF, jubilado, nos advirtió acerca de tratar el ciberespacio como un entorno puramente virtual: “El ciberespacio . . . es realmente un *dominio físico* resultante de la creación de sistemas y redes de información” (énfasis en el original).<sup>8</sup> El ciberespacio, claramente tiene una manifestación física en forma de dispositivos electrónicos usados para comunicarse, y el Coronel Rattray no iba descaminado al recordar a los guerreros de la información que no descontaran las interacciones físicas con el ciberespacio. No obstante, este argumento por sí solo no convenció a los individuos que trataron de elevar el ci-

berespacio a un dominio de combate maduro. Después de todo, ningún otro dominio fue definido por el equipo usado para operar dentro del mismo. Esto llevó últimamente a apropiarse el espectro electromagnético como la representación física del ciberespacio.

El Dr. Daniel Kuehl de la Universidad de Defensa Nacional—un defensor desde hace mucho tiempo de enlazar el ciberespacio estrechamente con el espectro electromagnético (ya se refirió a dicha relación a principios de 1997)—pasó a tener “una función importante en la creación” de la definición del ciberespacio del DOD en 2006.<sup>9</sup> Citado frecuentemente, sigue defendiendo esta definición centrada físicamente en el ciberespacio en documentos y como invitado en conferencias. La Fuerza de Tarea del Ciberespacio de la Fuerza Aérea de 2006, reflejando posiblemente estas primeras influencias y deseos de legitimar el ciberespacio, propuso un “credo cibernético”, que indicaba, entre otras cosas, que el “dominio cibernético es un *dominio de combate*. El espectro electromagnético es el espacio de maniobra” (énfasis en el original).<sup>10</sup>

La asignación del espectro electromagnético al ciberespacio es atractiva por una serie de razones. Ante todo, este espectro representa un fenómeno generalizado bien definido en el mundo físico, supuestamente preparado para sentarse en la misma mesa que los otros dominios físicos. La mayoría de las comunicaciones digitales, que intuitivamente parecen pertenecer al ciberespacio (si es que hay algo que pertenezca a él), se transportan en ondas de radio, microondas o rayos láser (ya sea de forma inalámbrica o mediante cables de fibra óptica), todos ellos pertenecientes al espectro electromagnético. Al usar esto como punto inicial, uno se encuentra que permitir que la definición del ciberespacio incluya cosas como el radar (una especie de información) y, con eso, contramedidas electrónicas, no parece completamente irracional. Súbitamente, el ciberespacio intenta un nivel de credibilidad completamente nuevo en la mente del combatiente tradicional si puede reclamar el campo relativamente venerable, demostrado y efectivo de combate electrónico como propio. Dado el empuje para establecer el ciberespacio como un nuevo dominio, uno puede fácilmente entender por qué el DOD adoptó inicialmente la definición física del ciberespacio de Kuehl.

No obstante, este método se encontró rápidamente con dificultades. Si el radar pertenece al ciberespacio, entonces, ¿por qué no el sonar? Después de todo, sirve esencialmente para lo mismo—en términos amplios—pero no saca provecho del espectro electromagnético de ninguna forma significativa. El láser en vuelo también es problemático por la razón contraria, ya que se basa casi completamente en el espectro electromagnético para crear efectos, pero cualquier definición del ciberespacio que incluya armas láser sería demasiado amplia y por ello casi inútil para fines prácticos. Prácticamente toda la inteligencia, la vigilancia y el reconocimiento; los sensores tácticos; y el ojo humano dependen del sistema electromagnético.

Aunque podemos caracterizar en gran medida el ciberespacio (lo definamos como lo definamos) mediante el uso de componentes electrónicos y el espectro electromagnético, al hacer eso se crean algunos problemas prácticos doctrinalmente. La asociación del espectro electromagnético con el ciberespacio conduce a reunir la guerra electrónica y, potencialmente, las operaciones de energía dirigida bajo el mismo paraguas que las operaciones de redes de computadoras. Esto resulta en la gestión de conjuntos de destrezas muy especializadas completamente distintas bajo una estructura a pesar de tener pocas cosas en común o ninguna en el adiestramiento y la doctrina. Además, desde un punto de vista teórico y doctrinal, los componentes electrónicos y el espectro electromagnético son en gran medida irrelevantes para la definición conceptual del ciberespacio, y su inclusión distrae de las características verdaderamente definitorias del ciberespacio.

Circunscribir el ciberespacio en términos de su uso de componentes electrónicos y del espectro electromagnético puede parecer algo intuitivamente evidente, pero sigue siendo una forma bastante superficial de describir el dominio. Después de todo, si el ciberespacio explotaba principalmente los efectos cuánticos del ciberespacio para procesar, almacenar e intercambiar información, ¿no seguiría siendo fundamentalmente igual desde una perspectiva de operaciones? Los mecanismos físicos usados por la tecnología empleada en el ciberespacio para producir

efectos no son características definidoras del dominio—no más que los carros de combate y la artillería son características definidoras del dominio terrestre.<sup>11</sup>

Ahora que el ciberespacio se ha establecido con éxito como una preocupación militar importante, las analogías forzadas con otros dominios han sobrevivido en gran medida su utilidad para hacer avanzar la teoría y la doctrina ciberespaciales. Según se observó antes, el DOD y la Fuerza Aérea se han alejado de un modelo de ciberespacio orientado físicamente, según se evidencia en la implementación de sus definiciones, organizaciones y procesos nuevos. Ya no tratamos la guerra electrónica como parte del ciberespacio, y basamos el desarrollo del adiestramiento y de la fuerza en una vista a centrada en redes de computadoras del dominio.<sup>12</sup> El naciente campo de profesiones de ciberguerra de la Fuerza Aérea consiste principalmente en personal de comunicaciones anterior.<sup>13</sup> La doctrina y el pensamiento de la ciberguerra parecen ir por el camino adecuado.

Desgraciadamente, hay una inercia considerable que sigue acompañando a los antiguos modelos de describir el ciberespacio—una situación entendible, dado el atractivo a las sensibilidades militares tradicionales. Hay documentos recientes que siguen refiriéndose y haciendo hincapié en los aspectos físicos del ciberespacio que tienen poco o nada que ver más allá de un nivel técnico o táctico, a pesar de tratar ostensiblemente de formular una teoría específica del dominio. En 2009, uno de estos tratados sobre la amenaza cibernética china se opuso explícitamente a la definición actualizada del ciberespacio del DOD (2008), recuperando el antiguo modelo orientado físicamente al observar que el ciberespacio también debe “comprender no solo los dispositivos electrónicos militares y civiles reales, sino también el espectro electromagnético por el que se desplaza la información”<sup>14</sup> El autor sigue adelante haciendo énfasis en que “en vez de eso las [operaciones de redes de computadoras] estrictamente independientes, la guerra electrónica y las operaciones espaciales se incorporarían dentro del dominio ciberespacial de gran alcance y etéreo, pero ‘físico’. De forma no diferente a los dominios de tierra, mar y aire”.<sup>15</sup> En 2011, un artículo de *Joint Force Quarterly* se refirió explícitamente al “ciberespacio (es decir, al espectro electromagnético)”.<sup>16</sup> Incluso el Documento de Doctrina de la Fuerza Aérea (AFDD) 3-12, *Cyberspace Operations (Operaciones ciberespaciales)* (2010), sigue mostrando el residuo de hacer énfasis excesivo en el espectro electromagnético aunque sigue el liderazgo del DOD pero sin igualar a los dos.<sup>17</sup>

El énfasis desmedido en los aspectos físicos del ciberespacio podría obstaculizar detalles claros difundiendo o circunscribiendo artificialmente el dominio, desviando potencialmente así más líneas aprovechables de pensamiento. El Dr. Samuel Liles, profesor asociado de la Universidad de Defensa Nacional, indica que “al concentrarse en un aspecto del ciberespacio (espectro electromagnético) se crea un punto ciego estratégico y conceptual para el liderazgo. También tienen una tendencia en concentrar la consideración del riesgo por medio de amenazas y vulnerabilidades sobre los mecanismos de transmisión”.<sup>18</sup> De forma correspondiente, la propagación continua de un paradigma del ciberespacio orientado físicamente refuerza estos puntos de vista defectuosos en las comunidades académica y, en cierta medida, operacional. El ciberespacio tiene claramente un elemento físico, pero las implicaciones son relativamente obvias, perteneciendo claramente a la doctrina existente para el ataque físico, la guerra electrónica y otras disciplinas muy trilladas. No obstante, el ciberespacio difiere fundamentalmente de otros dominios operacionales en una serie de formas que a veces desafían los intentos de establecer principios militares.

La identificación de las características realmente significativas y exclusivas de guerra en el ciberespacio ayudará a concentrar las mentes de teóricos, permitiéndoles avanzar de forma más eficiente en el campo determinando cómo la ciberguerra se desvía sustancialmente de la teoría y doctrina establecidas. Así, también pueden aclarar los principios de este dominio operacional relativamente nuevo y no familiar para el estratega y el comandante, ayudándoles a tomar decisiones más intuitivas a medida que operan dentro de él.

## El carácter exclusivo del ciberespacio

La capacidad de procesar, almacenar e intercambiar grandes cantidades de información rápidamente, usando sistemas automatizados, es la característica definidora del ciberespacio—los métodos físicos son superficiales. De hecho, su naturaleza lógica o virtual, en vez de sus mecanismos físicos, separan el ciberespacio de otros dominios. Esta característica lleva a una serie de implicaciones, algunas más evidentes que otras.

Quizás el atributo distintivo citado más a menudo de operar en el ciberespacio es su velocidad.<sup>19</sup> De hecho, la observación de que la ciberguerra tiene lugar “(casi) a la velocidad de la luz” se ha convertido en un estereotipo. Para la mayoría de los fines, las distancias físicas en el ciberespacio son casi insignificativas—solamente importan los asuntos topológicos. La planificación y preparación para un ataque puede llevar semanas o más en desarrollar la inteligencia y los accesos necesarios, pero, una vez lanzados, el ataque puede acabar en cuestión de segundos. En consecuencia, en muchos casos tal vez no seamos realistas para poder reaccionar a un ataque en curso. A menudo, un defensor no puede hacer nada más que negar los medios de ataque más dañinos por adelantado, activar la detección y responder rápidamente para mitigar y remediar sus efectos. Raramente se produce una confrontación entre fuerzas ofensivas y defensivas en tiempo real.

Esto aporta otro punto interesante. La ciberguerra es inusual en el sentido de que las fuerzas ofensivas y defensivas son muy asimétricas, comparadas con las de otros dominios.<sup>20</sup> Las fuerzas defensivas incluyen principalmente administradores de sistemas que supervisan varias redes, equipos de respuesta que llevan a rápidamente peritaje forense y soluciones, analistas de detección de intrusiones, y así sucesivamente, quizás junto con programadores de software que remiendan rápidamente defectos recientemente descubiertos, y compañías antivirus privadas que desarrollan firmas para inocular sistemas contra el nuevo malware.<sup>21</sup> Entretanto, las fuerzas ofensivas muy especializadas usan herramientas casi enteramente diferentes para atacar redes, a menudo tratando de no ser detectadas durante el tiempo que dure la operación. Dos fuerzas cibernéticas ofensivas opuestas no se encuentran en el ciberespacio para librar una guerra, como en otros dominios “cinéticos”; incluso si lo hicieran, los participantes no se encuentran ante un riesgo físico—un hecho que complica los esfuerzos para erosionar la capacidad de un enemigo para librar una ciberguerra.<sup>22</sup>

En *Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas)*, Martin Libicki de RAND explica con detalle la dificultad o imposibilidad de desarmar las capacidades cibernéticas de un enemigo: “De hecho, como los piratas informáticos solamente necesitan una computadora arbitraria y una conexión de red, no está claro que ni siquiera un ataque físico pueda destruir las capacidades de un ciberataque de un estado”.<sup>23</sup> Los haberes ofensivos irremplazables de un estado en una ciberguerra son sus piratas informáticos talentosos y su conjunto de éxitos. El estado puede mantener ambos bien protegidos contra un ataque físico y cibernético a menos que se vea tan abrumado que el resultado de la guerra ya no esté en duda. Incluso los sistemas de computadoras generalmente desechables usados por una fuerza cibernética del estado son difíciles de mantener en situación de riesgo mediante medios cibernéticos ya que pueden endurecerse mucho más efectivamente que una estación de trabajo o servidor típicos sin sacrificar la funcionalidad; además, en primer lugar, probablemente un asaltante tendría dificultades en detectarlos de forma precisa en la red. Una combinación de ataques físicos e inundación para cortar un estado completamente de la Internet podría denegar teóricamente sus fuerzas cibernéticas un medio de ataque (si no pueden reubicarse físicamente de forma encubierta a un aliado o tercera parte desconocida). No obstante, al hacer esto, se produciría un efecto recíproco impidiendo a los atacantes que penetraran en las redes del enemigo.

Todo esto implica que “el ciberespacio contraofensivo”, un término presentado sin comentario en AFDD 3-12, puede demostrar ser no significativo o al menos radicalmente diferente de la

ofensiva contraaérea (OCA), que utiliza claramente como modelo.<sup>24</sup> Aunque la definición estándar de la OCA es bastante amplia (y puede interpretarse que incluye ciber, al menos en cierta medida), normalmente pensamos en términos de disminuir la capacidad aérea ofensiva del adversario mediante la aplicación de su propia fuerza aérea.<sup>25</sup> Según se indicó arriba, tal vez no esperemos de forma realista disminuir sustancialmente una capacidad cibernética ofensiva del adversario mediante solamente medios cibernéticos ofensivos (o incluso medios cinéticos). Esto no significa que la capacidad cibernética ofensiva es inútil—meramente que estas fuerzas opuestas particulares no pueden afectarse significativamente, al menos no directamente ni en formas sugeridas por la OCA.

No solamente las fuerzas cibernéticas ofensivas siguen siendo inmunes al ataque, en su mayor parte, sino también las fuerzas defensivas pueden hacerse más fuertes durante el transcurso de una ciberguerra, incluso si va mal. Específicamente, los ataques de redes descubren vulnerabilidades que permiten de otra manera que los defensores reparen o mitiguen estos medios ofensivos de manera que las mismas herramientas del enemigo no puedan funcionar durante mucho tiempo. Como indica Libicki, un “atacante verá que es continuamente más difícil impactar blancos similares porque se protegen a medida que se recuperan de cada nuevo ataque”.<sup>26</sup> Así pues, las “ciberguerras” son muy perecedoras pero relativamente lentas y costosas de desarrollar, de modo que el potencial de ataque puede disminuir con el curso de una guerra.<sup>27</sup>

Entretanto, un comandante generalmente no tiene que aceptar vulnerabilidad para “amasar fuerzas” en otros lugares. Como las fuerzas ofensivas están probablemente separadas y son distintas de las fuerzas defensivas, en el ciberespacio no necesitamos considerar cómo asignar la capacidad de combate para “cubrir flancos” o intercambiar poder de fuego a fin de garantizar la seguridad de líneas de comunicación y retaguardias. Todos estos factores se combinan para sugerir que es posible que el desgaste no exista en la ciberguerra, al menos no en el sentido clásico.

Si las fuerzas cibernéticas no pueden llevar a cabo misiones de contrafuerza de forma realista dentro de su propio dominio, entonces la Fuerza Aérea debe cambiar la forma en que se aproxima a los objetivos bélicos en el ciberespacio en vez de en el aire. Según AFDD 3-01, *Operaciones contraaéreas*, “el control del aire es normalmente una de las primeras prioridades de la fuerza conjunta. Esto es especialmente así siempre que el enemigo sea capaz de amenazar fuerzas amigas desde el aire o inhibir la capacidad del comandante de fuerzas conjuntas (JFC) para llevar a cabo operaciones”.<sup>28</sup> El reemplazo del “aire” por el “ciberespacio” en este pasaje descubre cómo los aviadores podrían trazar un paralelo y llegar a la conclusión de que las fuerzas cibernéticas deben establecer prioridades para alcanzar la “superioridad del ciberespacio”. Esto puede ser posible en cierto sentido, pero puede simplemente significar ser mejor en el ataque y en la defensa que el enemigo. Esta declaración no es tan vacua como pudiera parecer a primer vistazo.

No aseguramos el “control del ciberespacio” llevando a cabo operaciones cibernéticas contra el adversario para debilitar sus capacidades mientras protegemos las nuestras; en vez de eso, desplegamos una fuerza capaz, bien adiestrada y con muchos recursos, con relación al adversario. Así pues, dicho control ya no es un objetivo operacional sino que también viene determinado en gran medida al principio de las hostilidades, como consecuencia de la planificación y preparación estratégicas durante tiempos de paz. Si participamos en una ciberguerra con fuerzas inferiores, no podemos depender de tácticas superiores para superar en maniobra al oponente, infringir mayores pérdidas y cambiar el curso (por varias razones descritas arriba). Así pues, “superioridad cibernética” se usa poco como término doctrinario porque su logro no es algo para lo que diseñamos campañas. En vez de eso, es un descriptor poco profundo de la calidad relativa de las fuerzas sobre las que los comandantes ejercerán poca influencia en tiempos de guerra. Si el enemigo claramente deriva una ventaja militar sustancialmente mayor del ciberespacio (es decir, tiene “superioridad”), un comandante puede tener solamente una palanca importante disponible: “saque” el ciberespacio hasta cierta medida, ya sea aislando sus fuerzas de la Internet

o haciendo lo mismo que el adversario mediante un ataque físico (o incluso lógico) —obviamente una medida drástica y más fácil de decir que de hacer.

## Conclusión

Como entorno de combate, el ciberespacio difiere fundamentalmente de los dominios físicos tradicionales, principalmente debido a su naturaleza lógica/virtual. Requiere tanto exámenes nuevos de los principios básicos como el aire, en relación a la guerra terrestre y marítima. Este carácter exclusivo reta muchas suposiciones sobre librar guerra. Si no podemos aplicar (directamente) dichos conceptos elementales como desgaste o contrafuerza a la ciberguerra, entonces debemos ser precavidos sobre tratar de forzar otros principios bélicos en la doctrina cibernética.

Hay pocos, si es que los hay, ejemplos claros de “ciberguerra” de los que podamos extraer lecciones demostradas de combate aprendidas.<sup>29</sup> En consecuencia, los individuos que crean la nueva doctrina gravitarán naturalmente a lo probado y comprobado en otros dominios y tratarán de injertar esos pedazos de sabiduría en esta nueva arena. Sin embargo, incluso si podemos justificar una forma de enlazar las operaciones cibernéticas con alguna estructura teórica venerada, hacer eso puede ser inútil si no da más detalles sobre como librar una guerra de forma eficaz. En vez de preguntarnos nosotros mismos la forma en que cierto principio se aplica a la cibernética, debemos preguntarnos primero si pertenece a la cibernética de alguna forma significativa. Solamente al evaluar de forma sincera las idiosincrasias del ciberespacio podemos aplicar de forma útil la sabiduría establecida y avanzar en la nueva doctrina. □

### Notas

1. Jeff Boleng, Dino Schweitzer y David Gibson, “Developing Cyber Warriors” (Desarrollo de los guerreros cibernéticos) (presentación, Tercer Congreso Internacional sobre guerra informática y seguridad, Academia de la Fuerza Aérea de EE. UU., Colorado Springs, CO, septiembre de 2007), <http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/boleng2008a.pdf>.

2. Cualquier observación sobre el congreso no citada en las notas son los recuerdos del autor, que asistió a él.

3. Departamento de Defensa, *The National Military Strategy for Cyberspace Operations (La estrategia militar nacional para las operaciones ciberespaciales)* (Washington, DC: Departamento de Defensa, diciembre de 2006), ix, [http://www.dod.mil/pubs/foi/joint\\_staff/jointStaff\\_jointOperations/07-F-2105doc1.pdf](http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf).

4. General de División Bill Lord, “Air Force Cyber Command (P) Update” (Actualización del cibercomando (P) de la Fuerza Aérea) (presentación, Asociación de Comunicaciones y Electrónica de las Fuerzas Armadas, Boston [Lexington-Concord chapter], 23 de enero de 2007), diapositiva 17, [http://www.afceaboston.com/documents/events/nh08/Gen\\_Lord.pdf](http://www.afceaboston.com/documents/events/nh08/Gen_Lord.pdf).

5. Presidente del Estado Mayor Conjunto, memorándum 0363-08, julio de 2008. Vea también la Publicación Conjunta (JP) 1-02, *Diccionario de términos militares y asociados del Departamento de Defensa*, 8 de noviembre de 2010 (según la enmienda hasta el 15 de agosto de 2012), 77, [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).

6. Es difícil demostrar una aseveración negativa, ya que la Fuerza Aérea evidentemente no tiene una declaración oficial que excluye explícitamente oficiales de sistemas de combate de las carreras cibernéticas o guerra electrónica en general del dominio del ciberespacio. No obstante, las referencias a dichos oficiales en las recientes publicaciones de la Fuerza Aérea sobre el ciberespacio parecen ser muy raras, escasas y sin desarrollar; además, el servicio generalmente parece tratar el ciberespacio como prácticamente sinónimo con sistemas de información y redes de datos—especialmente redes de computadoras basadas en el protocolo de Internet. No obstante, podemos declarar con seguridad que el campo de carreras 12R (oficial de sistemas de combate de guerra electrónica) permanece separado, no completamente integrado en el campo profesional de oficiales cibernéticos como se planificó inicialmente—a diferencia del campo profesional 33S (comunicaciones). Centro de Personal de la Comandancia de la Fuerza Aérea, *Directorio de Clasificación de Oficiales de la Fuerza Aérea* (Base de la Fuerza Aérea Randolph, TX: Centro de Personal de la Comandancia de la Fuerza Aérea, 1 de agosto de 2012), 48.

7. La Casa Blanca publicó unas guías en marzo de 2011 reduciendo las referencias públicas al ciberespacio como un dominio operacional militar a la par con la tierra, el mar, el aire y el espacio. Pero la propia existencia de dicha guía de alto nivel es un buen indicador que el campo de la ciberguerra está obteniendo más atención que antes. Casa Blanca, memorándum, tema: Guía de la Casa Blanca en lo referente al uso del “dominio” en Documentos sin clasificar y declaraciones públicas, 14 de marzo de 2011.

8. Gregory J. Rattray, *Strategic Warfare in Cyberspace (Guerra estratégica en el ciberespacio)* (Cambridge, MA: MIT Press, 2001), 17.

9. “La información como entorno puede ser un concepto difícil de entender, pero no hace falta discutir que hay un entorno físico al que la información está exclusivamente relacionada: ciberespacio. El ciberespacio es aquel lugar donde las computadoras, los sistemas de comunicación y esos dispositivos que operan por medio de energía radiada en el espectro electromagnético se encuentran y relacionan entre sí”. Dan Kuehl, “Defining Information Power” (Definición del poder de la información), *Foro estratégico*, no. 115 (junio de 1997): 3, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394366>. Vea también Kuehl, “The Information Revolution and the Transformation of Warfare” (La revolución de la información y la transformación de la guerra), en *The History of Information Security: A Comprehensive Handbook (La historia de la seguridad de información: manual completo)*, ed. Karl de Leeuw y Jan Bergstra (Amsterdam: Elsevier, 2007), 823n6.

10. Lani Kass, “A Warfighting Domain” (Un dominio bélico), 26 de septiembre de 2006, diapositiva 14, [http://www.au.af.mil/info-ops/usaf/cyberspace\\_taskforce\\_sep06.pdf](http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf).

11. “Reacciones químicas explosivas” es probablemente una analogía más cierta, aunque tal vez menos intuitiva. De forma muy parecida al espectro electromagnético frente al ciberespacio, es un fenómeno físico importante explotada manifiestamente al operar no solamente dentro del dominio terrestre sino también en los otros dominios.

12. El currículo de adiestramiento de aspirantes cibernéticos ofrece evidencia del enfoque sobre adiestramiento centrado en redes de datos. Julie R. Karr, “Cyberspace Force Development” (Desarrollo de la fuerza del ciberespacio), 18 de mayo de 2011, diapositiva 8, <http://www.safxc.af.mil/shared/media/document/AFD-110614-028.ppt>.

13. “30 de abril de 2010: [comunicaciones] personal/alojamientos 33S se convierten en [oficial cibernético] 17D. . . . 15 AFSC de [comunicaciones e información] realineados [códigos de especialidad de la Fuerza Aérea] en 11 AFSC 3DXXX [alistados cibernéticos]”. General de División David Cotton, “Cyberspace Workforce Transformation Update” (Actualización de transformación de la fuerza de trabajo del ciberespacio), mayo de 2010, diapositivas 14, 15. A pesar de esfuerzos en identificar miembros con talento de otros AFSC, particularmente en el cuerpo de oficiales, para que efectuaran la transición al campo profesional cibernético, los antiguos oficiales de comunicaciones siguen dominando numéricamente desde que se convirtieron en masa al nuevo AFSC, y el énfasis sigue estando en las habilidades de redes de computadoras.

14. Capitán de Corbeta Jorge Muñoz Jr., USN, “Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors” (Cómo cortar las uñas al dragón: por qué EE.UU. debe contrarrestar a los ciberguerreros chinos), (tesis, US Army Command and General Staff College, 2009), 2, <http://www.hsdl.org/?view&did=11694>.

15. *Ibid.*, 5.

16. Benjamin S. Lambeth, “Airpower, Spacepower, and Cyberpower” (Poder aéreo, espacial y cibernético), *Joint Force Quarterly*, número 60 (primer trimestre de 2011): 46, [http://www.ndu.edu/press/lib/images/jfq-60/JFQ60\\_46-53\\_Lambeth.pdf](http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf).

17. “[Cyberspace] requiere . . . énfasis en el espectro electromagnético . . . . Los sistemas también pueden diseñarse para cambiar frecuencias (los lugares donde operan dentro del espectro electromagnético) a medida que manipulan datos. Así pues, el espacio de maniobras físicas existe en ciberespacio”. Documento de doctrina de la Fuerza Aérea (AFDD) 3-12, *Cyberspace Operations (Operaciones ciberespaciales)*, 15 de julio de 2010 (incorporando el cambio 1, 30 de noviembre de 2011), 2, 3, <http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf>.

18. Samuel E. Liles, “An Argument for a Comprehensive Definition of Cyberspace” (Un argumento para una definición completa del ciberespacio), *Selil* (blog), 18 de noviembre de 2011, <http://selil.com/archives/2712>.

19. No hay escasez de referencias para esta idea, pero, por poner un ejemplo, AFDD 3-12 indica que “en el ciberespacio, el tiempo entre la ejecución y el efecto pueden ser milisegundos” y que las “operaciones pueden tener lugar casi instantáneamente”. AFDD 3-12, *Operaciones del ciberespacio*, 29, 9.

20. Uno debe observar la posible excepción del espacio, que tiene sus propias idiosincrasias que se salen del alcance de este artículo.

21. Este es un aspecto interesante del ciberespacio en su propio derecho—que las compañías privadas independientes podrían legítimamente considerarse parte de las fuerzas de defensa militares nacionales en cierta manera.

22. Se podría observar que ciertas operaciones de acceso podrían requerir que los miembros del equipo se pusieron en proximidad física a la red de un adversario, poniéndolos en riesgo. El autor arguye que esto constituye realmente soporte de operaciones especiales (o realización de) operaciones cibernéticas en vez de “fuerzas cibernéticas ofensivas” reales. Además, las fuerzas que las pondrían en riesgo físico ciertamente no eran fuerzas cibernéticas ofensivas.

23. Martin C. Libicki, *Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas)* (Santa Monica, CA: RAND, 2009), 60, [http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG877.pdf](http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf).

24. AFDD 3-12, *Cyberspace Operations*, 52. El ciberespacio contraofensivo también se identifica como la séptima de las nueve “áreas de capacidad cibernética de la Fuerza Aérea” en orden de prioridad. *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012–2025* (Washington, DC: AF/ST [Science and Technology], 15 de julio de 2012), 19.

25. La OCA comprende “operaciones para destruir, interrumpir o neutralizar aviones, misiles, plataformas de lanzamiento del enemigo y sus estructuras y sistemas de apoyo antes y después del lanzamiento, y tan cerca de su origen como sea posible. El objetivo de las operaciones de OCA es impedir el lanzamiento de los aviones y misiles enemigos destruyéndolos y su infraestructura de apoyo general antes el empleo”. JP 3-01, *Countering Air and Missile Threats (Cómo contrarrestar las amenazas aéreas y de misiles)*, 23 de marzo de 2012, I-3, [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_01.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf). “La

OCA incluye establecer objetivos . . . mando y control, comunicaciones, ciberespacio y nódulos de inteligencia enemigos". AFDD 3-01, *Counterair Operations (Operaciones contraaéreas)*, 1 de octubre de 2008 (cambio provisional 2 [última revisión], 1 de noviembre de 2011), 5–6, <http://www.e-publishing.af.mil/shared/media/epubs/afdd3-01.pdf>.

26. Libicki, *Cyberdeterrence and Cyberwar (Disuasión y guerra cibernéticas)*, 59.

27. Libicki explora este concepto con más detalle en *ibid.*, 56–59. Habla de la posibilidad de que una guerra cibernética “disminuya paulatinamente” a medida que los ataques se hacen menos efectivos con el tiempo (*ibid.*, 135).

28. AFDD 3-01, *Counterair Operations (Operaciones contraaéreas)*, 1.

29. En varios casos aislados, han tenido lugar operaciones cibernéticas (por ejemplo, supuestamente durante la Operación Huerto y el gusano Stuxnet, también conocido como Juegos Olímpicos). No obstante, estos no llegan a guerra abierta en el dominio cibernético (aunque podrían servir muy bien como modelo sobre la forma en que los ataques cibernéticos se usan más comúnmente en la realidad—operaciones encubiertas de precisión). Algunos individuos pueden discutir que el ciberataque ruso en Georgia en 2007 representa un “buen ejemplo de ciber guerra”—quizás el más claro hasta la fecha. De todas formas, en este caso la disparidad entre los dos lados hace difícil decir si el aspecto cibernético del ataque tuvo cualquier impacto significativo en el conflicto. Se hace difícil defender que este ejemplo es una base para la doctrina de la ciber guerra.



**El Mayor Sean C. Butler, USAF** (BS, University of Southern California; MS, Air Force Institute of Technology) forma parte del cuerpo docente de la Escuela Superior de Comando y Estado Mayor de la Fuerza Aérea, Base Aérea Maxwell, Alabama. Obtuvo su nombramiento a través del Cuerpo de Adiestramiento de Oficiales de la Reserva de la Fuerza Aérea en la University of Southern California. El Mayor Butler prestó servicio en el 23er Escuadrón de Operaciones de Información, Base Aérea Lackland, Texas, donde estuvo a cargo de diseñar tácticas de guerra en la red. En calidad de profesor auxiliar que dirigió y dictó el curso de seguridad en la red en la Academia de la Fuerza Aérea, guió un grupo de cadetes a que ganaran el Ejercicio de Defensa Cibernética 2004 en el que participaron otras academias de los demás servicios armados. En la Academia, fue uno entre un grupo de expertos en la materia de la Fuerza Aérea seleccionado a poner a prueba operacional en el 2007 el curso de Entrenamiento de Guerra en la Red y ayudó a desarrollar el plan de estudio que se convirtió en la base del entrenamiento actual de la fuerza cibernética de la Fuerza Aérea.



---

## Reseña de Libros

---

**El Cociente del Liderazgo: 12 Dimensiones para Medir y Mejorar el Liderazgo** (The Leadership Quotient: 12 Dimensions for Measuring and Improving Leadership) por Bill Service y Dave Arnott. Universe Press (<http://www.iuniverse.com>), 2021 Pine Lake Road, Suite 100, Lincoln, Nebraska 68512, 2006, 496 páginas, US \$30.95.

Un libro interesante e importante, *The Leadership Quotient* (*El Cociente del Liderazgo*) proporciona un modelo realista, práctico y factible para identificar, medir y mejorar la efectividad del liderazgo. Los autores Bill Service y Dave Arnott sostienen con lógica sólida y convincente que los líderes deben entender claramente los fundamentos y la interacción de seguidores, líderes y entornos. Esta interacción es esencial para convertirse en un líder de éxito. Aunque no ha surgido ninguna definición simple y aceptada universalmente de liderazgo, los autores hacen eco correctamente de la definición más ampliamente aceptada entre los teóricos y practicantes: el liderazgo es cualquier intento de influenciar el comportamiento de un individuo o grupo para lograr un objetivo.

Service y Arnott afirman que no hay magia en ser un buen líder, sugiriendo que el liderazgo efectivo incluye invertir tiempo en cosas que son realmente importantes, establecer prioridades, medir resultados y premiarlas. No siendo un trabajo motivador tradicionalmente simplista, según los números, ni un tratamiento académico de las teorías y análisis del liderazgo, *The Leadership Quotient* bosqueja los principios básicos de un conjunto de pautas lógicas para medir y mejorar el liderazgo propio a través del entendimiento más profundo y la aplicación de las herramientas de liderazgo. Sosteniendo que toda persona tiene el potencial de ser líder, proporciona un modelo de cuatro cuadrantes para que los individuos identifiquen e influyencen sus cualidades personales de liderazgo para mejorar sus capacidades como líderes o ayudar a otros a serlo.

Este texto que empieza por lo básico es muy convincente en sostener que se deben aprender y practicar los fundamentos del liderazgo sin importar el nivel de liderazgo que ocupe la persona en el momento o el nivel al que aspire. En efecto, la gente no va a la escuela una vez en la vida para estudiar liderazgo sino que permanecen en la escuela toda la vida. Lo que aprendan después de saber todo es lo que realmente cuenta. Además, los momentos de aprendizaje ocurren a medida que las personas se van convirtiendo en líderes: las cosas ocurren una y otra vez, y ellos aprenden en una espiral, no en línea recta. Así, un día llegan a ser líderes.

Un estilo de vida para el éxito en liderazgo, *The Leadership Quotient* clasifica y mide los puntos fuertes y débiles del líder con el fin de mejorar el desempeño sostenible del liderazgo. Los autores identifican 12 dimensiones verificables de liderazgo calificadas como cocientes, midiéndolas por separado y de forma interactiva: apariencia, comportamiento, comunicaciones, deseo, emociones, inteligencia, conocimiento, gerencia, gente, realidad, situación y experiencia. Esta fórmula para mejoramiento del liderazgo está diseñada para perfeccionar la ejecución del liderazgo de cualquiera que tenga seguidores en condiciones de entornos variables. Service y Arnott claramente definen estos cocientes mientras guían a los lectores por el proceso de acceder a su habilidad para liderar, creyendo que llegar a ser líder significa primero ser uno mismo mediante el autodescubrimiento. Su libro apoya directamente el desarrollo del liderazgo centrando al estudiante en la auto-reflexión y en encontrar la esencia del liderazgo a través de una evaluación personal guiada.

Este estudio concienzudo y que provoca la reflexión también aborda el compromiso y la necesidad del liderazgo dirigida hacia el logro. Los líderes no pueden ayudar a cambiar el presente porque el presente no es suficientemente bueno. Los autores establecen un punto excelente indicando que el título de líder es solo una frase. En realidad, uno gana reputación como líder obteniendo la confianza, comprometiéndose a algo distinto que el interés propio y ayudando a otros a lograr sus metas. Adicionalmente, en el Apéndice A, los autores nos ayudan a entender que el liderazgo y la gerencia, aunque relacionados, son diferentes.

Específicamente, la gerencia se otorga mientras que el liderazgo se gana. No obstante, los dos se apoyan: necesitamos líderes y gerentes.

Examinar *The Leadership Quotient* es una experiencia gratificante: Este revisor está convencido de que los líderes que aplican con éxito sus principios avanzarán mucho en la solución de problemas que puedan tener consigo mismos, sus seguidores o las situaciones que confronten.

**Dr. Richard I. Lester**  
Maxwell AFB, Alabama

**Morir para Ganar: La Lógica Estratégica del Terrorismo Suicida** (Dying to Win: The Strategic Logic of Suicide Terrorism) por Robert A. Pape. Random House (<http://www.randomhouse.com/rhpg>), 1745 Broadway, New York, New York 10019, 2005, 352 páginas, US \$25.95 (tapa gruesa), \$14.95 (tapa delgada).

En *Dying to Win* (*Morir para Ganar*), el profesor Robert Pape sostiene que a pesar de la difundida creencia sobre lo contrario, el fundamentalismo islámico no es la causa raíz del terrorismo suicida. Más bien, el 95 por ciento de tales ataques entre 1980 y 2003 ocurrió como parte de campañas coherentes que tenían objetivos políticos y territoriales, no religiosos. De acuerdo con la tesis del autor, “El terrorismo suicida es principalmente una respuesta a la ocupación extranjera” (pág. 23). Aunque esto parezca una proposición más bien limitada, si se valida, podría debilitar de forma significativa muchas otras explicaciones populares de este fenómeno, tales como globalización, un choque de civilizaciones, e Islam contra la democracia.

El Dr. Pape presenta considerable evidencia para apoyar su tesis. Estudiando sistemáticamente 315 ataques suicidas que ocurrieron durante un período de 23 años, demuestra que la mayoría de ellos no fueron actos aislados llevados a cabo por fanáticos solitarios que deseaban morir por Islam. Presenta un buen caso de que las acciones de los Tigres Tamil, Hamas e incluso al-Qaeda fueron campañas guiadas racionalmente, impulsadas por problemas sobre la ocupación extranjera (u ocupación percibida) de territorio. El hecho de que bombarderos suicidas individuales puedan no ser racionales no significa que ellos no puedan ser parte de un esquema racional más grande. Islam juega un rol en el reclutamiento de potenciales atacadores suicidas, pero no es el único ni incluso el factor primario.

Un problema con el libro es su oportunidad, relacionada con la situación actual en Irak. Según la Brookings Institution, ocurrieron más ataques suicidas en Irak desde el 2003 (la fecha de publicación del libro) que los que tuvieron lugar globalmente en los 23 años previos. Esto deja un número grande de incidentes que no analiza el estudio.

Un segundo problema incluye el hecho de que el autor no aborda suficientemente la idea del estado islámico. Si los grupos terroristas buscan restablecer tal estado, como bin Laden clama con frecuencia, entonces el terrorismo es más que simplemente combatir la ocupación extranjera de territorio. El establecimiento de un estado islámico universal quiere decir que la distinción entre extranjeros y nativos resulta mucho menos importante que aquella entre musulmanes y no musulmanes.

La obra del Dr. Pape saca a flote interrogantes importantes acerca del rol del territorio como causa del terrorismo suicida. Podría socavar la noción que los terroristas son actores irracionales más allá del compromiso. Como lo señala, los terroristas continúan realizando ataques suicidas porque las democracias del mundo siguen haciendo concesiones después de tal uso (por ejemplo España). Si estos actos son parte de estrategias racionales para la liberación nacional, entonces no ayudará reorganizar el mundo musulmán a lo largo de líneas democráticas. Los terroristas simplemente verían a la democracia como otra forma de ocupación extranjera que no tendría ningún efecto en detener los ataques, e incluso podría provocar más ataques. Sea que uno concuerde o no con la tesis del Dr. Pape, todos los legisladores y estudiantes de relaciones internacionales deberían leer *Dying to Win*.

**Capitán Jason Belcher, USAF**  
Goodfellow AFB, Texas