

AIR & SPACE **POWER** JOURNAL en ESPAÑOL

Volumen 25, N° 3

TERCER TRIMESTRE 2013



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

Editorial	2
La Guerra Aérea en Libia Mayor Jason R. Greenleaf, USAF	4
Funciones de Inteligencia, Vigilancia y Reconocimiento en Vuelo con Operadores Humanos Mayor Tyler Morton, USAF	21
La Aviación y el Espacio Cibernético—Convergencia de Ámbitos, Convergencia de Amenazas Emilio Iasiello	32
Murió la Contrainsurgencia: ¿Qué más? Remy Mauduit	40
Ataque Conjunto Inteligente en el Ciberespacio Mayor Steven J. Smart, USAF	43
Profesionales Cibernéticos en las Fuerzas Armadas y en la Industria Transcrito por el Capitán Jeffrey A. Martínez, USAF, y el Capitán Matthew R. Kayser, USAF	54
Fronteras Nuevas, Realidades Antiguas Dr. Everett Carl Dolman	65
Justificación de un Comando Combatiente del Ciberespacio Teniente Coronel Shawn M. Dawley, Air National Guard	78
Sin Lugar Para Esconderse: La Creciente Amenaza Para Las Bases Aéreas Coronel Shannon W. Caudill, USAF Mayor Benjamín R. Jacobson, USAF	86



Editorial

Un análisis objetivo sobre las Operaciones Odyssey Dawn y Protector Unificado, ejecutadas en Libia con la finalidad de proteger a sus civiles y cuyos resultados en ese momento se tradujeron en el éxito de la campaña aérea liderada por Occidente, llevaron al Mayor Jason R. Greenleaf a plantearse en su artículo “La Guerra Aérea en Libia”, la premisa concluyente de que a pesar del resultado exitoso de esa operación emprendida por la coalición, no puede desconocerse la difícil situación resultante al no haber sido abordadas oportunamente muchas de las cuestiones operativas, realidad ésta que hay que tener presente ante similares operaciones futuras.

El Mayor Tyler Morton, en su artículo “Funciones de Inteligencia, Vigilancia y Reconocimiento en Vuelo con Operadores Humanos (ISR)”, describe el cambio y evolución de las funciones tradicionales de ISR basado en los mayores conflictos del pasado, y hace énfasis en la conveniencia de las funciones de recopilación de inteligencia a nivel estratégico que han convertido a la comunidad ISR en el primer proveedor mundial de inteligencia a nivel táctico. Haciendo referencia a la Fuerza Aérea y, sin desconocer su rol tradicional de recopilación de información de tipo estratégico, el autor insiste en la necesidad de mantener sus capacidades tácticas dentro de sus funciones ISR, para lo cual considera exigente en los aviadores, el aprendizaje de habilidades lingüísticas, analíticas e informativas, enfocadas estratégicamente.

A medida que la tecnología digital evoluciona y su uso se multiplica y se torna cada vez más común, se incrementan también en forma significativa y simultánea las amenazas de ataques cibernéticos contra una aeronave, instalación, o medios de comunicación, requiriéndose entonces la implementación oportuna de mayores medidas de seguridad. Teniendo en cuenta esta realidad, el Sr. Emilio Iasiello en su escrito sobre “La Aviación y el Espacio Cibernético”, considera que la aviación civil y militar no están aún preparada para defenderse de esta catastrófica amenaza y necesita de manera preventiva adelantarse al problema y tomar medidas contra estas amenazas cibernéticas.

Situándose en la historia y con una óptica retrospectiva respecto a las operaciones de contrainsurgencia (COIN) no muy exitosas y, siendo realista en el análisis sobre las lecciones aprendidas en Afganistán e Irak, Rémy Mauduit en su escrito “Murió la Contrainsurgencia: ¿Qué más?”, cuestiona seriamente el valor e intención de dichas operaciones y sostiene que en el futuro deberíamos evitar este tipo de guerras y pensar seriamente en la insurgencia como la razón fundamental de la forma más frecuente de conflictos y tener un mayor entendimiento de sus causas y objetivos.

El tema de la aplicación de las leyes de la guerra y la doctrina militar existente en lo que se refiere a la selección de blancos para operaciones militares en el ciberespacio, es abordado por el Mayor Steven Smart en “Ataque Conjunto Inteligente en el Ciberespacio”, quien después de explorar la eficacia de la aplicación de la actual *Publicación Conjunta (JP) 3-60, Selección Conjunta de Blancos*, y reconociendo que la ciberguerra difiere fundamentalmente del conflicto armado tradicional, recomienda una actualización de la *JP 3-60* que incorpore una doctrina conjunta y una guía específica para la selección de blancos en el recién reconocido ámbito cibernético.

Teniendo como referencia una conversación entre dos de los mejores líderes cibernéticos de nuestra nación, a través de la cual se examinan las oportunidades y las vulnerabilidades cada vez mayores del ámbito cibernético, los Capitanes Jeffrey Martínez, y Matthew R. Kayser, en su aporte titulado “Profesionales cibernéticos”, se pronuncian respecto a la responsabilidad compartida entre el gobierno y la industria en la defensa de la nación. Este diálogo pone de manifiesto la magnitud de los cambios organizativos y tecnológicos necesarios para instituir una transformación a nivel empresarial, teniendo en cuenta las lecciones aprendidas de esta iniciativa exitosa, que debe servir de soporte técnico a la Fuerza Aérea y a la industria en sus esfuerzos por aplicar en un futuro los principios de la ciberseguridad.

Las implicaciones geopolíticas como consecuencia del armamentismo y del control del espacio ultraterrestre, así como también el inminente peligro de una guerra espacial entre Estados Unidos y China, en el afán de lograr una superioridad espacial, son aspectos analizados objetivamente por el Dr. Everett Carl

Dolman en “Fronteras Nuevas, Realidades Antiguas”. El autor sostiene que la opción de desplegar armas en el espacio y la creciente preocupación por evitar una nueva hegemonía espacial se traducirá en una costosa carrera armamentista y desestabilizadora, que podría evitarse mediante la implementación por parte de ambas naciones, de un tratado internacional que prohíba el uso de armas espaciales.

La consideración de designar al Comando del Ciberespacio de los Estados Unidos (USCYBERCOM), recientemente formado como un comando combatiente, es tema de análisis por parte del Teniente Coronel Shawn Dawley, quien en su artículo “Justificación de un Comando Combatiente del Ciberespacio”; argumenta que ante las amenazas contra Estados Unidos y sus aliados presentadas por la implementación del armamentismo en el Ciberespacio y la posibilidad de una ciberguerra, sería de mayor interés para la seguridad nacional el contar con un Comando combatiente del Ciberespacio con la requerida autoridad que le permita desarrollar, emplear y explotar capacidades dentro de este reciente campo de acciones de guerra.

Finalmente, al analizar las crecientes amenazas de que son blanco las bases aéreas y las operaciones espaciales, los autores del artículo “Sin lugar para esconderse”, el Coronel Shannon W. Caudill y el Mayor Benjamín R. Jacobson, argumentan con razón que el riesgo para los medios aéreos y espaciales, puede convertirse exponencialmente más complejo y que el costo de las contramedidas puede incrementarse debido a la promulgación de la tecnología, la abundancia de información de código abierto, y el avance del conocimiento y experiencia del enemigo. Una creciente vulnerabilidad de todo el espectro de peligros causados por la tecnología y las capacidades emergentes, harán que las defensas de los medios aéreos sean aún más difíciles. En consecuencia, la alta probabilidad de estos riesgos emergentes y los costos asociados para garantizar las operaciones aéreas continuas, debe constituirse en una consideración prioritaria y muy cuidadosa por parte de los aviadores.



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

La Guerra Aérea en Libia

MAYOR JASON R. GREENLEAF, USAF

Una actitud aún más peligrosa que asumir que una guerra futura será la última, es imaginar que será tan diferente que podemos darnos el lujo de hacer caso omiso de todas las lecciones de la última.

—Sir John C. Slessor, *El poder aéreo y los ejércitos*, 1936



YA HA PASADO MÁS de un año desde que concluyó la última misión aérea Operación Protector Unificado de la Organización del Tratado del Atlántico Norte (OTAN).¹ En solo algo más de siete meses, la campaña aérea dirigida por Occidente (vea la figura N°1), iniciada como respuesta a la resolución del Consejo de Seguridad de las Naciones Unidas (UNSCR) para proteger a los civiles libios, permitió a un grupo de rebeldes desorganizados conseguir la derrota de un ejército bien armado y la caída de una dictadura que se prolongó durante más de 40 años. Desde el final de la misión, han tenido lugar pocos debates o análisis públicos de la campaña. Aunque sigue habiendo algo de escepticismo en lo que se refiere al futuro de la nación norteafricana, rica en petróleo, un consenso abrumador de opinión considera que la guerra aérea en Libia ha sido un éxito completo y un ejemplo de lo que puede lograr una operación liderada por la coalición. Tomas Valasek, del Centro de Reforma Europeo en Londres, afirma que fue “una de las mejores guerras que puede haber”.² Los diplomáticos de Estados Unidos y Europa están de acuerdo con esta evaluación, describiendo de forma similar los méritos de la guerra en superlativos. No obstante, antes de considerar la imitación de los esfuerzos de la coalición en otra intervención, es prudente y necesario hacer una revisión y un escrutinio deliberados. Además, un análisis completo revela que estas evaluaciones no tratan de muchos problemas de operación que demostraron ser difíciles y que necesitan un examen adicional, incluidas las relaciones con implicaciones del poder aéreo general y preocupaciones clave. Al final, aunque la campaña pueda haber alcanzado sus objetivos estratégicos, operacionalmente debe servir de muchas formas como una señal de alarma para todas las personas involucradas.

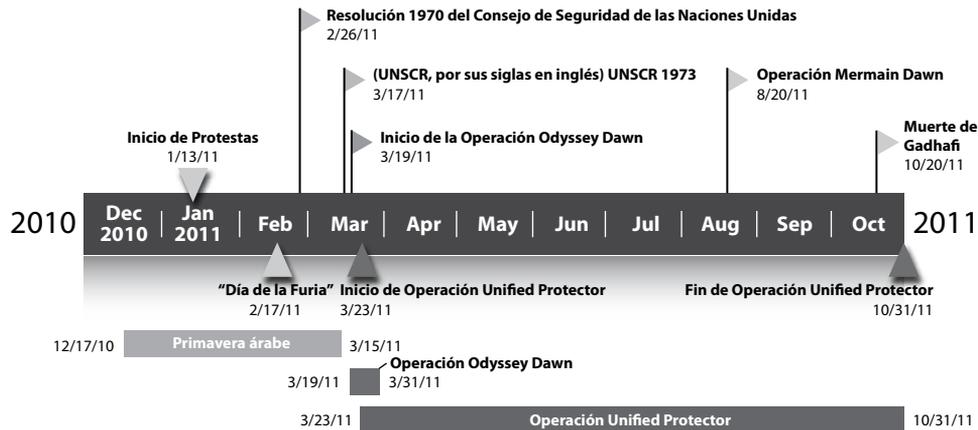


Figura N°1. Línea cronológica de la campaña aérea libia. La Operación Unified Protector consistía de tres elementos. El 23 de marzo de 2011, la OTAN comenzó el embargo de armas y el 25 de marzo el cumplimiento de una zona de no vuelo. El 31 de marzo, la OTAN se apoderó del control de todas las operaciones militares, inclusive la protección de civiles de ataques o amenazas de ataque. (“Operation Unified Protector: Final Mission Stats” (Operación Unified Protector: Estadísticas de la misión final), NATO .int, 2 de noviembre de 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2-11_11/20111108_111107-fact-sheet_up_factsfigures_en.pdf.)

Operación Odisea del Amanecer

Para aquellos que dudaban de nuestra capacidad de llevar a cabo esta operación, deseo dejarlo claro: Estados Unidos de América ha hecho lo que dijo que iba a hacer.

—Presidente Barak Obama

Desde el comienzo, Estados Unidos no quiso asumir el liderazgo durante la crisis en Libia. El Secretario de Defensa Robert Gates aconsejó no establecer una zona de exclusión aérea; incluso después de que empezara la Operación Odisea del Amanecer, insistió en que el conflicto de Libia no era un interés vital para Estados Unidos.³ A pesar de esta reserva inicial, la Fuerza de Tarea Conjunta de Odisea del Amanecer siguió adelante el 3 de marzo de 2011, comenzando las operaciones aéreas el 19 de marzo. Casi inmediatamente después, Estados Unidos empezó a trabajar de forma diligente para transferir el control de la campaña a la OTAN.⁴ Hacia el 31 de marzo, dicha organización había asumido la máxima responsabilidad de la misión, en la que Estados Unidos adoptó una función auxiliar secundaria en Protector Unificado, y Odisea de Amanecer se dio por concluida. A pesar de la brevedad de la operación—menos de dos semanas de combate real—dejó claras muchas deficiencias, tanto tácticas como estratégicas. No obstante, este hecho no debe desmerecer la hazaña impresionante de organizar una fuerza de tarea conjunta, concentrándose en una coalición de 15 naciones participantes a pesar de una guía estratégica rápidamente variable, llevando a cabo 2.000 misiones para obtener una supremacía aérea, y transfiriendo las operaciones a otra organización—todo eso en menos de un mes. Como comandante del componente aéreo de la fuerza conjunta, el General de División Margaret Woodward, USAF, recordaría más adelante, “La historia está clara . . . la operación tuvo un gran éxito”.⁵ No obstante, de no captar las mejoras que es necesario que tengan lugar, se cometería una injusticia con los involucrados en este conflicto y las futuras acciones saldrían perjudicadas.

Lecciones de EE.UU. identificadas

El Comando de África de EE.UU. (AFRICOM), al que se le encomendó la tarea de liderar la operación, se vio plagado de deficiencias organizativas desde un principio. El Secretario Gates resaltó sin saber estas insuficiencias durante la activación del comando en 2008, observando que la “misión de AFRICOM no es librar una guerra, sino prevenirla”.⁶ El comando combatiente geográfico más reciente, encargado inicialmente de las tareas de evacuación de no combatientes y reorientado después a una operación cinética, tuvo dificultades en ejecutar una misión que nunca intentó llevar a cabo.⁷ El estado mayor de pequeña dotación (300 personas) nunca había practicado operaciones de fuerzas de tarea conjuntas con sus comandos de componentes; tampoco podría servir su centro de operaciones aéreas (AOC) como algo que no sea “un comando de transporte para apoyar a personal y hacer transferencias de materiales dentro del (teatro de operaciones)”.⁸ En vez de eso, AFRICOM tuvo que fiarse en gran medida en personal, instalaciones y conocimientos expertos del Comando Europeo para ejecutar la misión con éxito. AFRICOM, organizado, adiestrado y equipado solamente para llevar a cabo el enfrentamiento en el teatro de operaciones, luchó para organizar una campaña aérea en el último minuto.⁹ La dirección estratégica en rápido desarrollo y la escasez de recursos complicó la capacidad del comando de llevar a cabo la misión, pero las limitaciones externas también impidieron el curso de las operaciones.¹⁰

El General Woodward reconoció rápidamente las carencias y limitaciones a las que se enfrentó con la capacidad orgánica a su disposición. A medida que la misión pasó de ser una operación de evacuación de no combatientes, a una zona de exclusión aérea y una obligación de proteger civiles, el alcance y la sensación de urgencia también aumentaron. No obstante, la administración de fuerzas globales/solicitud de procesos de fuerzas no pudieron mantener esta sensación de urgencia que los servicios usan para distribuir, asignar y destinar fuerzas y “obtener el apoyo requerido que no se haya asignado ya al comando”.¹¹ Aun cuando la primera y única solicitud de fuerzas se envió pronto y “fue validada casi inmediatamente por AFRICOM y el Estado Mayor Conjunto, la aprobación de estos recursos simplemente no se produjo a tiempo para las operaciones”.¹² Este deseo de recursos demostró ser la limitación más difícil en el desarrollo de la estrategia de la campaña aérea.¹³ Particularmente negativa fue la ausencia de aviones críticos como el Sistema Aerotransportado de Control y Alarma (AWACS) E-3, el Sistema de Radar de Ataque de Objetivos de Vigilancia Conjunta (JSTARS) E-8 y aviones cisterna adicionales que posiblemente deben haber estado allí primero pero no llegaron hasta después de que empezaran las operaciones de combate.¹⁴ Además, como los haberes de inteligencia, vigilancia y reconocimiento (ISR) que poseían un video de movimiento completo no estaban disponibles hasta que la OTAN se hizo cargo de la misión, los pilotos encontraron dificultades para distinguir a los rebeldes de las fuerzas leales a Muamar el Gadafi e identificar objetivos sensibles en función del tiempo. De hecho, después de que las fuerzas pro Gadafi abandonaran sus equipos convencionales, la diferenciación entre las dos fuerzas sin haberes de ISR persistentes que pudieran desarrollar una información de pautas de comportamiento demostraron ser casi imposibles. Junto con UNSCR 1973, que limitaba el empleo de fuerzas terrestres de la OTAN, la carencia de ISR inhibió una evaluación exacta de los daños de batalla y desembocó en ataques adicionales a “objetivos que podrían haberse neutralizado ya”.¹⁵ La incertidumbre sobre la disponibilidad de los haberes y su llegada al teatro de operaciones también afectó el uso eficiente de la aviación de los planificadores.

La decisión de considerar el establecimiento de bases para todos los aviones que llegan al teatro de operaciones pareció fortuita y no usó de forma efectiva el número limitado de haberes de reabastecimiento de combustible aéreo disponibles.¹⁶ La inmensidad de Libia, aproximadamente del tamaño de Alaska, y la falta de campos de aviación adecuados cercanos a la zona de exclusión aérea aumentó el tiempo de tránsito e hizo que casi todos los haberes se basaran en el

reabastecimiento de combustible aire a aire. Las decisiones del establecimiento de bases resultaron en poner aviones caza cerca del conflicto a expensas de aviones pesados. En consecuencia, para permanecer en la estación, estos últimos necesitaban un avión cisterna para cada salida. A continuación se produjo un dilema clásico, ya que los planificadores tenían que escoger entre reabastecer de combustible las plataformas de comando y control (C2) pesadas/ISR o los haberes de ataque. Los relativamente pocos haberes de ISR, objetivos planificados de antemano, y la necesidad moral de minimizar los daños colaterales significaba que la mayoría de los ataques tenía que usar objetivos dinámicos así como tácticas de coordinación y reconocimiento para buscar y destruir fuerzas pro Gadafi.¹⁷ Por su propia naturaleza, estas dos misiones hacen que los haberes de ataque dependan de administradores de batallas aéreas a bordo de plataformas C2 pesadas.¹⁸ Los planificadores a menudo tenían suficiente combustible para los aviones que podrían acoplar disparadores con objetivos o para los disparadores mismos—pero raramente para ambos. Una vez que haya empezado un esfuerzo de planificación deliberado, los oficiales de enlace y planificadores hicieron cambios que maximizaban la efectividad de los recursos limitados. Claramente, esta operación subrayó la importancia del reabastecimiento de combustible aéreo y de la obtención de acceso a las bases. No obstante, la tiranía de la distancia y la complejidad relacionada de las decisiones de las bases en este teatro de operaciones no eran fenómenos nuevos. Los planificadores deben haber identificado y mitigado estos problemas mucho antes.¹⁹

Se puede decir lo mismo de las barreras de comunicación entre las fuerzas aliadas. El General Carter Ham, EE.UU., comandante de AFRICOM, alaba el nivel de interoperabilidad y la coordinación durante *Odisea del Amanecer* como el “ideal” que las operaciones futuras deben tratar de alcanzar.²⁰ No obstante, en toda esa operación y en Protector Unificado, varios problemas impidieron las operaciones. Entre los más importantes estaban el uso de sistemas clasificados para comunicarse con la OTAN, un problema que obstaculizó el reparto de información. Las fuerzas de EE.UU. utilizaron la SIPRNET (Red de Routers de Protocolos Secretos de Internet) para planificar y ejecutar *Odisea del Amanecer*, pero la OTAN no tiene acceso a este sistema, usando en su lugar sus Operaciones de Respuesta Secretas y de Crisis en los Sistemas Operativos (CRONOS) de la OTAN para transmitir información secreta.²¹ Aunque el sistema de recopilación de información y explotación del campo de batalla (BICES) emergió a finales de los años 80 para rellenar este hueco, no estaba ampliamente disponible para las fuerzas de EE.UU. y “no existía en AFRICOM”.²² La ausencia del BICES complicó la transferencia a la OTAN, especialmente durante las primeras etapas de Protector Unificado. Hasta que el sistema se hizo disponible en lugares de escala para haberes de EE.UU., no existía ningún medio seguro para transmitir la orden de tareas aéreas y otra información de la misión. Así pues, los oficiales de enlace podían transferir la información básica de las salidas solamente a las tripulaciones, que después tendrían que comprobar con la agencia aérea C2 durante el resto de su pedido de tareas aéreas. Además, los problemas de compatibilidad no se limitan al personal en tierra.

Surgió otro problema al averiguar las capacidades detalladas de la aviación de la coalición. La mayoría de los haberes pertenecían a las naciones de la OTAN, pero no existía un mecanismo para diseminar información básica de todos los participantes en lo que se refiere a sus capacidades de aviación. La falta de familiaridad de los planificadores con la radio, el enlace de datos y otros equipos de aviación seguros de cada nación tuvo un efecto negativo en el desarrollo de un plan de comunicaciones, el establecimiento de prioridades y la resolución de conflictos de frecuencias, y la planificación de las contingencias de búsqueda y rescate. Estados Unidos no solo sufrió una escasez de sistemas compatibles con sus socios sino que también tuvo problemas en hacer que los sistemas se comunicaran ya que el “estándar de la OTAN” no demostró ser ni un estándar ni ser siquiera accesible a los haberes de EE.UU. Este tema aplicado a la carga de criptología en radios y otros dispositivos para hacerlos seguros así como a metodologías de empleo como la función desempeñada por haberes tácticos C2 como el AWACS.²³

Implicaciones de las fuerzas de EE.UU.

Afortunadamente, la mayoría de las grietas identificadas en la operación de EE.UU. se prestan a una resolución rápida. Estados Unidos debe tratar las deficiencias de las estructuras organizativas de comandos combatientes geográficos. Según el General Ham, “Los comandos combatientes no tienen ocasión de escoger sus misiones”.²⁴ Si van a tener las mismas responsabilidades y autoridades que otros comandos, entonces necesitamos relacionar recursos y conjuntos de misiones apropiados. Odisea del Amanecer ejemplifica cómo ciertos comandos no están organizados por tareas para ejecutar la gama completa de misiones de combate pero puede esperarse que lideren durante las operaciones de contingencia inesperadas con sus límites geográficos. En el caso de esta operación, decidir quién lideró la misión basándose en líneas de un mapa en vez de en capacidades causó mucha confusión y consternación. Sin las fuerzas de operación asignadas, salvo las de la Séptima Fuerza Aérea y la Fuerza de Tarea Conjunta–Cuerno de África, la transferencia de la misión después de evolucionar y convertirse en una operación cinética a gran escala habría demostrado ser más eficiente. El Comando Europeo, que terminó de proporcionar la mayor parte de la infraestructura, la dotación, los equipos y los conocimientos expertos, habría sido una opción lógica. El Departamento de Defensa debe considerar cuidadosamente si todos los comandos combatientes geográficos tendrán las capacidades para llevar a cabo operaciones menores y mayores o si debe continuar con ciertos comandos de “misión limitada”. La desactivación de la Decimoséptima Fuerza Aérea el 25 de abril de 2012 puede reflejar las inclinaciones de personas que toman decisiones estratégicas.

Además, la gestión de la fuerza global/solicitud de procesos de fuerzas exige un examen y un refinamiento adicionales. El movimiento hacia las cadenas de suministro esbeltas y una mentalidad “justo a tiempo” limitan la flexibilidad de operaciones. A pesar del éxito durante la ejecución de una operación de tiempo crítico dentro de un entorno limitado por recursos, la Fuerza Aérea de EE.UU. podría asignar completamente haberes para solamente cuatro de los 90 requisitos, una situación probablemente exacerbada por las realidades políticas porque el Congreso no aprobó esta operación.²⁵ Aunque el despliegue de haberes no depende de dicha aprobación, su ausencia revela la dificultad de responder rápidamente en cualquier lugar del mundo.²⁶ Esto también resalta un peligro real de basarse demasiado en lo que la Fuerza Aérea llama la “fuerza de apoyo electrónico”, que se “refiere a basarse en la aviación de combate y apoyo de EE.UU. . . . o al personal de apoyo basado en CONUS [Estados Unidos continentales] ligado electrónicamente a unidades de vanguardia”.²⁷ El General Woodward se hizo eco de este sentimiento, advirtiendo que Odisea del Amanecer debe servir como “una señal de alarma”.²⁸ Gran parte del crédito va a las capacidades y al profesionalismo del personal de servicio que realizó la misión con las pocas fuerzas que tenía a mano, pero podemos descubrir que durante la siguiente contingencia operar de esta manera no sería suficiente o se demoraría mucho. Estados Unidos puede hacer mucho para asegurarse de que su infraestructura y sistemas activen los haberes adecuados para acudir al lugar adecuado a tiempo disminuyendo la dependencia en la fuerza de apoyo electrónica y refinando la gestión de la fuerza global/solicitud para procesos de fuerzas.

Además, EE.UU. debe la normalización de los equipos e integrarlos con los de los miembros europeos de la OTAN. Es increíble que los miembros de la mayor alianza militar del mundo sigan desarrollando y desplegando sistemas incompatibles. Aun cuando Estados Unidos actualiza sus plataformas C2/ISR con capacidad de conversación segura por Internet aire a tierra, la versión de EE.UU. (conocida como mIRC) no es compatible con la versión de la OTAN (JChat).²⁹ Objetivos, prácticas y limitaciones políticas diferentes pueden impulsar a las naciones a distintas fuentes de compras diferentes, pero deben estar de acuerdo al menos en las normas que hacen que los sistemas sean operables entre sí. Un servicio puede retener sistemas específicos también basados solamente en EE.UU., pero debe tener los mismos medios de operación que los socios de la OTAN. La ausencia de los componentes estándar de la OTAN prescritos por acuerdos nor-

malizados socava la ya tenue capacidad de la asociación para luchar incluso bastante cerca de Europa. En su mayor parte, Estados Unidos ha superado problemas relacionados con las comunicaciones y la cooperación entre sus servicios pero debe ampliar esa normalización a los socios de la OTAN. En 2010, el Comando Europeo reconoció la necesidad de emplear el BICES rápidamente en todo el teatro de operaciones ya que “otros países de la OTAN han estado usando el sistema durante años”; no obstante, el AOC poseía solamente un terminal de BICES.³⁰ Aun cuando el personal usara equipos compatibles, el acceso limitado a una criptología estándar disponible significaba que, en muchos casos, tenían que usar palabras codificadas para pasar información sensible acerca de frecuencias de radio claras. La transmisión de un mensaje de establecimiento de objetivos de 10 líneas de forma segura entre fuerzas que hablan el mismo idioma lleva relativamente mucho tiempo. Al hacer esto entre individuos que posiblemente no hablen bien inglés o tengan muchos acentos diferentes se detiene el proceso por completo.

Por último, la confianza y la familiaridad inherentes entre socios involucrados a los niveles operacional y táctico parecía faltar o al menos se desarrolló lentamente. Muchos países no querían integrarse completamente desde un principio y limitaron su interacción con elementos de apoyo de otras naciones. Por ejemplo, debido en gran medida a su política de neutralidad, Suecia no se había enfrentado en combate ni siquiera se había desplegado operacionalmente durante más de 50 años antes de Protector Unificado.³¹ Ciertamente, nadie cuestiona la capacidad de combate de las fuerzas suecas, pero evidentemente tuvieron dificultad en integrarse sin esfuerzos en operaciones de combate de la OTAN. Para eliminar esta duda y aumentar la confianza mutua, debemos hacer ejercicios regionales y un adiestramiento más realista e inclusivo. La participación en ejercicios de la OTAN o de la coalición no dirigidos por EE.UU. identificará áreas para la mejora y cualquier restricción en un entorno de adiestramiento. No obstante, Estados Unidos ha mostrado repetidamente que la mera identificación de lecciones no resolverá el problema ya que pasa por alto u olvida rápidamente muchas de ellas. En 2000, la Fuerza Aérea envió un informe completo por RAND que identificó los “problemas de interoperabilidad potenciales que pueden surgir en las operaciones de la Alianza de la OTAN o en las operaciones de la coalición de EE.UU. con los aliados de la OTAN durante la siguiente década” y ofreció soluciones para mitigar esos problemas.³² No obstante, durante la ejecución de Odisea del Amanecer, muchos de estos retos siguieron siendo claramente rodeos exigentes en tiempo real. Tanto el General Ham como el General Woodward afirmaron con razón que esta operación fue un “ejemplo de adiestramiento, ejercicios e interoperabilidad diarios que hemos formado con varios socios en todo el mundo”, pero en la ejecución—especialmente durante las primeras fases—hay muchas cosas que mejorar.³³

Operación Protector Unificado

La operación ha hecho visible que los europeos carecen de una serie de capacidades militares esenciales.

—Secretario General de la OTAN Anders Fogh Rasmussen

Lecciones de la OTAN identificadas

Protector Unificado fue la primera operación aérea importante de la OTAN desde la Fuerza Aliada de Operación de 1999 en los Balcanes y la primera vez que los europeos se hicieron con el liderazgo, donde Estados Unidos acordó asumir una función de apoyo.³⁴ Una operación que empezó con mucho escepticismo y muchos defectos terminó predominando, haciendo declarar a algunos que era un modelo de futuras intervenciones.³⁵ Otros sintieron que la operación representaba una “lección confusa para la OTAN”, exponiendo fisuras en la alianza y lagunas en

las capacidades.³⁶ Sea cual sea el resultado de estos debates, la OTAN debe enfrentarse a algunos problemas claros, tanto estratégicos como tácticos.

Protector Unificado sufrió una falta de cohesión estratégica en lo que se refiere a que menos de la mitad de las naciones miembro contribuyeron a la operación.³⁷ Descontando la participación de EE.UU. y Canadá, solamente seis países europeos suministraron una capacidad ofensiva. A luz de la Fuerza Aliada, que disponía de fuerzas de 14 de los 19 miembros de la alianza, no es de extrañar que algunas personas pongan en cuestión la capacidad de la OTAN de actuar al unísono y cuestionar lo que significa para la identidad de la seguridad futura. El verano pasado el Secretario Gates criticó fuertemente a la OTAN, afirmando que se había deteriorado y que era una estructura de miembros de dos niveles “entre los que desean y pueden pagar el precio y llevar la carga de los compromisos, y los que disfrutaban de las ventajas de ser miembro de la OTAN pero no desean compartir riesgos y costos”.³⁸ Algunas de las naciones que se abstuvieron podrían haber participado pero simplemente decidieron no participar en el conflicto.

Además de dicha falta de determinación, Protector Unificado puso al descubierto limitaciones significativas en la habilidad militar de la alianza. En general, muchos líderes europeos utilizaron a la OTAN como un medio de asegurar la participación de EE.UU. y obtener “capacidades exclusivas” que no se encuentran en ningún lugar de la alianza.³⁹ Estados Unidos relleno los huecos en las plataformas de ISR, aviones de reabastecimiento de combustible en el aire y aviones a control remoto. Aunque EE.UU. tripuló solamente el 25 por ciento de las salidas, siguió suministrando la mitad de los aviones, tripuló el 80 por ciento de las misiones de reabastecimiento de combustible en el aire y de ISR, y aumentó el C2 aéreo con el 25 por ciento de cobertura y control.⁴⁰ El resto de ISR provino principalmente del Reino Unido y Francia, lo que también ascendió a la mitad de las fuerzas de ataque—reflejando nuevamente la falta de presión de reparto entre participantes.⁴¹ La OTAN también dependía de Estados Unidos en casi todas las misiones de supresión de defensa área del enemigo así como en búsqueda y rescate en combate.⁴² Simplemente, sin el apoyo significativo de Estados Unidos, a los socios europeos se les habría hecho muy difícil llevar a cabo esta operación con el éxito con que lo hicieron.

Incluso los haberes suministrados por las naciones europeas no podrían sostener operaciones de combate a largo plazo. Inicialmente, la OTAN esperó una acción libia a corto plazo, pronosticando operaciones solamente hasta julio. Dicha organización merece reconocimiento por pasar sucesivamente dos prolongaciones de tres meses, pero aun cuando podría haberse creído preparada para un largo plazo, las fuerzas y los suministros de la OTAN no lo estaban. A principios de junio, salieron a la luz informes de que varias naciones se estaban quedando sin armas, de modo que Estados Unidos tuvo de recomponer su inventario de armas agotadas.⁴³ Poco después, Noruega, que había contribuido el 17 por ciento de las misiones de ataque con solo seis aviones, anunció que retiraría sus fuerzas debido a la excesiva carga involucrada.⁴⁴ (Esto no debería distraer de la contribución de Noruega. Esa nación, junto con Dinamarca y Bélgica, “tripuló un porcentaje de las misiones mucho mayor en proporción al tamaño de sus fuerzas aéreas”, aumentando aún más la disparidad de reparto de obligaciones entre los miembros europeos de la OTAN).⁴⁵ Las 26,500 salidas durante la campaña pueden parecer significativas hasta que se tenga en cuenta que en los 78 días de la Fuerza Aliada, la coalición tripuló más de 38,000 salidas, de las 15,000 que correspondían a miembros que no eran EE.UU.⁴⁶ Lo que fue aún más preocupante durante Protector Unificado es que las operaciones aéreas fueron diseñadas “para un esfuerzo de 300 salidas al día pero . . . tuvo dificultad[es] en conseguir 150”.⁴⁷ El hecho de que una “operación muy pequeña” puso a la alianza en dificultades resulta intranquilizador.⁴⁸

Además de la falta de ciertos haberes aéreos, la conducción de las operaciones en tierra demostró ser más difícil que lo anticipado. Algunos oficiales superiores dicen que las fuerzas hicieron una “transición suave” desde *Odisea del Amanecer* liderada por EE.UU. a Protector Unificado liderada por la OTAN, pero otros oficiales involucrados en la operación disputan esta

afirmación, aseverando que ese “momento se perdió durante la transición al control de la OTAN”.⁴⁹ De hecho, solamente debido a las instalaciones deficientes del centro de operaciones aéreas combinadas (CAOC) la transición habría sido cualquier cosa menos una transición sin problemas. El CAOC en Poggio Renatico, Italia, no tenía infraestructura para apoyar el puñado de personas asignadas permanentemente allí en CAOC 5, y menos aún a los cientos de oficiales de enlace y otro personal de apoyo que llegaron a la base. En unos pocos días, sus instalaciones temporales estaban a rebosar. Inmediatamente después, la OTAN no parecía debidamente organizada ni tenía recursos para asumir el control de la operación.

El comando y el control de la campaña había hecho una transición del AOC de la Fuerza Aérea de EE.UU. con una infraestructura robusta de comunicaciones e informática a otra sin equipos para una operación de este alcance. Las pocas radios que se podían asegurar de la coalición (solamente se disponía de dos radios de comunicación por satélite rudimentarias con microteléfonos para llevar a cabo las operaciones) complicaron los nuevos problemas de los equipos del CAOC. Como los haberes de EE.UU. no gozaban de la capacidad de JChat, casi todas las comunicaciones aéreas—tanto críticas con respecto al tiempo como administrativas—tenían que usar solamente dos frecuencias disponibles. Emergieron problemas adicionales de interoperabilidad de equipos: los teléfonos seguros en las instalaciones del AOC no podían comunicarse con teléfonos seguros de EE.UU. en sus bases, y ningún bando podía tener acceso a la capacidad del otro. La instalación especial construida para los oficiales de enlace de EE.UU. les dio acceso a SIPRNET, comunicaciones de satélites y teléfonos seguros para hablar con sus homólogos de EE.UU. pero aún así siguieron sin poder comunicarse con el CAOC, que estaba a unos pocos cientos de metros. Como observó el autor, había mensajeros que tenían que ir de un lugar a otro cuando el personal de las instalaciones del CAOC no podía ponerse en contacto con un haber aéreo con los medios disponibles, o viceversa.

Las diferencias de ejecución de *Odisea del Amanecer* a Protector Unificado no proceden meramente de instalaciones inadecuadas; también reflejaban los programas de adiestramiento respectivos y estructura de C2. Durante *Odisea del Amanecer*, Estados Unidos se sobrepuso a la falta de experiencia del personal por medio de procesos de capacitación normalizados conocidos para cada persona asignada a un AOC.⁵⁰ En su mayor parte, cada AOC de EE.UU. tiene las mismas funciones, procesos e incluso un documento de guía que abarca tácticas, técnicas y procedimientos.⁵¹ Aunque Estados Unidos invierte un tiempo y unos esfuerzos considerables capacitando a su personal de AOC, la OTAN no lo hace. Debido a su estructura organizativa y procesos internos, la OTAN no tiene fuerzas permanentes a su mando, y la generación de fuerzas no empieza hasta que el Consejo del Atlántico Norte apruebe el concepto de operaciones.⁵² El paso siguiente—la adquisición de haberes y personal—requiere tiempo para la coordinación de toda la alianza de la OTAN, dando apoyo a la observación del Capitán de Corbeta Dave Ehredt de que la “OTAN no destaca por su velocidad o agilidad para responder a una crisis internacional”.⁵³ Debido al plan de transición acortado y al sistema lento y deliberado de la OTAN, el CAOC en Italia necesitó un aumento importante de personal de EE.UU.—específicamente especialistas en objetivos.⁵⁴ Nuevamente, el autor observó que el personal de la OTAN al trabajar con las funciones de CAOC en las instalaciones no tenía experiencia ni adiestramiento ni estaba capacitado para hacerlo.

Los problemas con los equipos y el personal adiestrado en CAOC acrecentaron los problemas relacionados con las advertencias nacionales en una estructura de coalición. Cualquier coalición tiene reglas de enfrentamiento, procesos de aprobación y niveles de daños colaterales distintos que cualquier nación esté dispuesta a aceptar. Protector Unificado no comprendía ninguna regla permanente de la coalición, por lo que la decisión definitiva sobre si de debía atacar o no un objetivo no se producía normalmente en la cabina del piloto sino atrás, en el CAOC, y la tomaban los “encargados de las tarjetas rojas” de las naciones—oficiales superiores consultados durante el proceso de selección de objetivos. Esta capa adicional de toma de decisiones complicaba

aún más las demoras resultantes de la criptología incompatible, barreras de idiomas y confianza en el establecimiento de objetivos dinámicos y tácticas de coordinación y reconocimiento de ataques. A menudo, el bajo nivel de combustible obligó a un haber de ataque a volver a la base después de haber esperado más de 30 minutos para la aprobación de enfrentarse a un objetivo hostil, dejándolo a veces intacto. Antes, en Protector Unificado, estas demoras contribuían probablemente a quejas rebeldes de que la campaña aérea de la OTAN no estaba haciendo lo suficiente para desgastar las fuerzas del régimen.⁵⁵

Implicaciones para la OTAN

Muchos de los problemas surgidos durante la operación de la OTAN liderada por los europeos no tendrán una solución sencilla. La dificultad que experimentó la organización en su intento de obtener el consenso para una operación legalmente validada por UNSCR 1973 y considerada políticamente legítima a través del apoyo de la Liga Árabe plantea cuestiones sobre la unión de los miembros europeos de la OTAN alrededor de una identidad de defensa común.⁵⁶ Algunos expertos perciben la operación como un “símbolo del éxito de EE.UU. para convencer a sus aliados de que los europeos tienen que asumir un mayor porcentaje de la carga y asumir una mayor responsabilidad para la seguridad en Europa y su periferia”.⁵⁷ De hecho, aunque fue prometedor ser testigo de que el Reino Unido y Francia asumieran el liderazgo diplomático en la operación, la transición a la OTAN sirvió únicamente para resaltar la falta de capacidades que Estados Unidos trata de aprovechar en el futuro.

Tanto los socios europeos de la OTAN como Estados Unidos deben tratar la diferencia de capacidades que existe en Europa y su dependencia de EE.UU. Algunos analistas pueden elogiar las mayores capacidades de los países europeos citando la proporción relativa de salidas o armas gastadas por socios de la OTAN que no son EE.UU. y de la coalición, pero incluso “el avión caza más avanzado es de poco uso si los aliados no tienen los medios para identificar, procesar y atacar objetivos como parte de una campaña aérea integrada”.⁵⁸ Estos no son extras opcionales en una campaña aérea; son cosas esenciales que, en el presente, solamente Estados Unidos parece capaz de proporcionar.⁵⁹ Incluso con las capacidades actuales de los miembros europeos, deben invertir más en armas y apoyo para asegurarse de que las operaciones tengan éxito en futuros conflictos. La Fuera Aliada nos enseñó que las carencias de municiones guiadas por precisión plantean una amenaza al éxito general de la misión.⁶⁰ En la mucho menor operación libia, volvió a surgir problema y pronto. Cuando la OTAN asumió el control, la defensa aérea y la amenaza área integradas libias ya se habían eliminado, por lo que los aviones de la OTAN disfrutaron de un entorno permisivo desde el comienzo. Aún así, el anticuado sistema de defensa de Gadafi y la fuerza aérea mínima probablemente habría presentado un reto sobrecogedor a los europeos solamente. La OTAN dependía de Estados Unidos no solo en lo que se refiere a haberes aéreos sino también para establecer objetivos y personal, sin el cual la operación habría demostrado ser mucho más problemática. El Secretario de Defensa Leon Panetta se hizo eco de la advertencia de su predecesor a los líderes europeos de que Estados Unidos ya no puede absorber y cubrir las limitaciones de la alianza.⁶¹

Estados Unidos y los socios europeos de la OTAN, al enfrentarse a crisis económicas graves, están cambiando la práctica del pasado de gastar de forma opulenta y están tratando de minimizar sus inversiones en defensa. Algunas naciones, seguras de que no pueden permitirse el lujo de una espectro máximo de capacidades, parecen moldear sus fuerzas suponiendo que otros suplirán la diferencia. Al final, los participantes de la alianza pueden proteger sus objetivos de seguridad respectivos aprovechando las capacidades de otros—lo cual se puede materializar o no en el futuro. Dada la dependencia de la estrategia de seguridad nacional de EE.UU. en el apoyo de la alianza, el tamaño de las fuerzas decrecientes del Reino Unido y de otras, los dos niveles apa-

rentes de miembros de la OTAN, y una crisis económica global, la posibilidad de repartir carga para la seguridad colectiva parece más intimidadora que lo que se podría haber anticipado.

Entretanto, la OTAN debe buscar soluciones innovadoras así como refinar estructuras y procesos actuales para encontrar soluciones de costo bajo y alto rendimiento. Puede hacer eso mejorando la capacitación y rescribiendo publicaciones para que se puedan alinear con las prácticas reales de los estados miembro. Varios miembros de la OTAN tienen grandes necesidades, y otros se enfrentan a déficits fiscales, incluida la crisis de la deuda de EE.UU. La alianza no puede permitirse el lujo de invertir en tecnologías diversas o en doctrina incompatible entre naciones miembro que requieran un apoyo mutuo. La OTAN debe considerar también seriamente fusionar y reorientar la arquitectura C2 alejándose más de su diseño legado de la Guerra Fría.⁶² En vez de mantener varios CAOC más pequeños con una capacidad limitada, la alianza haría mejor en concentrarse en una o dos instalaciones debidamente dotadas, adiestradas y equipadas para operaciones de combate modernas. La OTAN ha tomado las medidas para reducir algunas de sus redundancias y arquitectura, pero el diseño actual sigue presentando un desajuste de capacidades y ambiciones siempre que el concepto estratégico mantenga operaciones “fuera del área”.⁶³

La OTAN también se beneficiaría considerablemente de un programa de adiestramiento similar al de Estados Unidos—uno que normalice el adiestramiento para el personal asignado a CAOC. Por último, aunque todas las naciones que participan en futuras operaciones probablemente no estarán de acuerdo por completo con las reglas de enfrentamiento o con la cantidad de daños colaterales aceptables, podrían desarrollar y codificar una norma por adelantado para impedir las demoras experimentadas en Libia. Esto podría adoptar la forma de matrices de opciones que el representante de un país acepta desde el principio—por ejemplo, Norma de la OTAN Regla de enfrentamiento 1a, CDE B, que informa a los planificadores y operadores a quienes se les pueden asignar tareas y a qué objetivos.⁶⁴ Estos cambios ayudarán a reducir la fricción involucrada en las primeras fases de la operación y hacen que la fuerza sea más efectiva desde el comienzo. En el futuro, es posible que la alianza no tenga el lujo de tratar con un adversario que permita una respuesta gradual en escalada.

Lecciones e implicaciones del poder aéreo

Para bien o para mal, el dominio del aire es hoy en día la expresión suprema del poder militar, y aunque las armadas y los ejércitos, son vitales e importantes, deben aceptar un rango subordinado.

—Winston Churchill, 1949

Desde el principio de la operación libia, los expertos y eruditos de todo el mundo empezaron a postular y profetizar lo que significaría esta operación para el poder aéreo. Dado que las fuerzas terrestres de la coalición no participarían, Odisea del Amanecer ofreció una probabilidad de determinar finalmente si el poder aéreo podría alcanzar la victoria por sí solo. No obstante, al final, la operación no produjo resultados claros pero sugirió muchas conclusiones diferentes.

Los puntos clave en lo que se refiere al uso del poder aéreo en Libia son importantes en muchos aspectos. Primero, el entorno y las circunstancias asociadas con la guerra son probablemente representativos de conflictos en un futuro próximo. Libia ofreció a los defensores de la intervención un nuevo método para lograr resultados deseables cuando se justifica la misión de “responsabilidad de proteger”.⁶⁵ Los conflictos futuros también comprenderán probablemente pequeñas alianzas. Las naciones estarán menos inclinadas a llevar a cabo operaciones unilaterales, y la coalición que se desarrolle comprenderá una amplia variedad de socios con distintas capacidades y advertencias nacionales. En segundo lugar, a la luz de la reciente guerra terrestre

en Irak y la retirada que viene de Afganistán, las alianzas probablemente no estarán de acuerdo en compromisos grandes de tropas en un futuro próximo.

El poder aéreo ofrece una opción de respuesta rápida, relativamente económica, que se puede aumentar en escala y de bajo riesgo para líderes políticos. A pesar de todas las conversaciones sobre gastos de misiles de crucero y bombas inteligentes, estos elementos del poder aéreo siguen siendo una fracción del costo que supone desplegar un ejército. Por último, a medida que las naciones de todo el mundo se enfrentan a disminuciones inevitables en gastos militares, deben tomar decisiones difíciles sobre los programas que desean mantener. Algunos observadores postulan que los resultados de Libia auguran buenos tiempos para las fuerzas aéreas de todo el mundo mientras que otros sugieren que las operaciones mostraron que es posible que estas fuerzas no merezcan la inversión.

Algunos críticos concluyen que el poder aéreo no pudo cumplir con la promesa de producir resultados decisivos sin el apoyo de un componente terrestre fuerte.⁶⁶ Muchos teóricos determinaron pronto que el régimen de Gadafi se derrumbaría de forma bastante rápida bajo un ataque de la coalición, pero resistió siete meses.⁶⁷ El régimen ciertamente parecía dirigirse a la derrota rápida durante la primera oleada de ataques que destruyeron la defensa aérea libia, inmovilizaron la fuerza aérea y volaron sin oposición en los primeros días. Pero después “la primera alianza militar del mundo y los tres ejércitos más formidables del mundo” apenas prevalecieron “sobre un déspota de tercera categoría”.⁶⁸ Si los libios, cuyos gastos de defensa eran un ocho por ciento de los de la oposición, casi forzaron un empate con la alianza occidental, entonces esta campaña tal vez no sea un buen ejemplo de la promesa del poder aéreo.⁶⁹

Para tratar las acusaciones de que el poder aéreo no había sido decisivo, los proponentes reclaman que no alcanzó resultados abrumadores contra Libia debido a limitaciones militares y políticas que relegaron el poder aéreo a opciones tácticas en vez de a objetivos estratégicos.⁷⁰ En vez de atacar nudos de comunicación y centros de mando, los aviones tuvieron que llevar a cabo la tarea laboriosa e ineficiente de destrucción de objetivos con municiones guiadas, como en Kosovo durante Fuerza Aliada.⁷¹ Muchas personas lamentan que dicha asignación convierte “una fuerza aérea en una rama de artillería excesivamente costosa.”⁷²

Además, el entorno político en rápida evolución impidió a los jefes aéreos de la OTAN que recibieran objetivos claramente definidos. Según el General Charles Horner, USAF, retirado, que lideró la campaña aérea de la coalición en Operación Tormenta del Desierto, “Para tener éxito, los líderes militares necesitaban objetivos claramente definidos que pueden lograrse mediante el uso de la fuerza”.⁷³ Muchos defensores del poder aéreo consideraban que el UNSCR estaba muy limitado en términos de lo que podían lograr las fuerzas aéreas. La misión nebulosa de “proteger a los civiles” no aclaró hasta que punto iba a llegar la alianza ofensivamente contra las fuerzas pro Gadafi. Inicialmente, fue aparente que la alianza necesitaba detener su avance hacia el baluarte rebelde de Bengasi, pero después de eso la misión se hizo más ambigua.⁷⁴ La OTAN adoptó después un método más graduado y coercitivo que al principio no se fijó como objetivo la capacidad militar de Gadafi ni trató de cambiar el régimen.⁷⁵

Este método limitado fue criticado por los que buscaban un “dominio rápido” del poder aéreo y una victoria acelerada y decisiva, pero aseguró probablemente el éxito de la misión porque los rebeldes podían haber explotado esta ventaja inicial.⁷⁶ Al extenderse la guerra e igualarse las condiciones para las fuerzas rebeldes, el poder aéreo dio al Consejo de Transición Nacional el tiempo necesario para organizar y aglutinar en vez de crear un vacío de poder. Tal vez, entonces, aunque no sea glamoroso, el poder aéreo en Libia hizo exactamente eso lo que se suponía que tenían que hacer. La Fuerza Aérea de EE.UU. ha afirmado desde hace mucho que la fuerza del poder aéreo se basa en su flexibilidad y capacidad de escala. Entre otras formas de poder militar, solo el poder aéreo puede mantener simultáneamente una serie de objetivos en riesgo y “proporciona un espectro de opciones de empleo con efectos que van de lo táctico a lo estratégico.”⁷⁷

Sean cuales sean las evaluaciones eventuales de las operaciones aéreas en Libia, una cuestión que surgió y sigue sin contestar es la definición del término *poder aéreo*. El documento de la doctrina básica de la Fuerza Aérea lo describe como “la capacidad de proyectar el poder militar o influir a través del control y de la explotación del aire, espacio y ciberespacio para lograr objetivos estratégicos, operacionales o tácticos”.⁷⁸ Claramente ausente de esta definición es cualquier mención de suministrar efectos cinéticos, indicando que el poder aéreo consiste más en disparar misiles y dejar caer bombas. La OTAN pareció tener suficientes haberes de ataque pero demostraron ser deficientes en aviones de ISR, aviones cisterna y aviones con piloto remoto. Los haberes de ataque de la OTAN, mostraron la versatilidad y capacidad de adaptación del poder aéreo, cumplieron algunos de los requisitos de ISR desempeñando las funciones de recopilación de ISR no tradicionales como las reglas de enfrentamiento desarrolladas para cada nación. No obstante, muchos individuos siguieron disputando que el número limitado de posibilitadores dentro de las naciones europeas de la OTAN refleja lagunas significativas de lo que constituye el poder aéreo. El hecho de que los submarinos lanzaran una barrera de misiles de crucero para destruir los nudos de defensa aérea clave describe el punto en que el poder aéreo incluye algo más que la aviación convencional.⁷⁹ Esto parece demostrar que en Libia, “el uso real del poder aéreo . . . resalta el hecho de que el ‘poder aéreo’ no es necesariamente lo mismo que la fuerza aérea del país”.⁸⁰

Muchas personas pueden afirmar correctamente que las naciones más pequeñas no podrán nunca permitirse el lujo de una gama completa de capacidades que conforman el “poder aéreo”, un hecho que exige una atención más concentrada en las capacidades especializadas que contribuyen a la mayor fuerza de la OTAN. Si los miembros europeos de la OTAN prefieren la especialización, y la integración y el reparto de equipos para una defensa común, entonces deben lograr mayores grados de coordinación. Asegurar la adquisición de los haberes correctos y el adiestramiento y equipamiento adecuados de personal listo para acoplarse a la estructura del poder aéreo general representa una empresa enorme que exige una cooperación política sustancial.

Aunque podemos decir que el “poder aéreo” decidió la campaña contra Libia, está menos claro lo que realmente significa. Sin duda, los servicios y programas que vean reducciones en sus presupuestos tratarán de aprovecharse de esta ambigüedad al tratar de conseguir los recursos adicionales. Estados Unidos y las fuerzas de la OTAN involucradas en Odisea del Amanecer y Protector Unificado pueden extraer y aportar lecciones claras de planificación y ejecución de la campaña. No obstante, para los defensores de cualquier lado del debate de supremacía del poder aéreo, las implicaciones generales siguen siendo inciertas. Sería difícil restar importancia a la ventaja asimétrica que el poder aéreo de la coalición dio a los rebeldes; al mismo tiempo, el estancamiento de la campaña aérea de la OTAN pone legítimamente en cuestión su aplicación exclusiva. Claramente la coalición y su uso del poder aéreo no proporcionaron una plantilla de operación óptima para futuros conflictos pero probablemente informará de futuras decisiones tácticas, de adiestramiento y transformación. Aunque los líderes militares y políticos siguen elogiando la campaña como una solución militar ejemplar de bajo riesgo, la guerra contra Libia no resolvió de forma conclusiva la noción de la preeminencia del poder aéreo en la guerra; de hecho, parece haber confundido el entendimiento tradicional de lo que incluso significa el poder aéreo. La campaña tampoco indicó claramente cómo las naciones deben conformar su fuerza durante el período inevitable de austeridad presupuestaria. Cien años después de que el capitán italiano Carlo Piazza volara por primera vez sobre Libia, parece que Odisea del Amanecer/Protector Unificado no nos ha acercado más a responder algunas de estas preguntas eternas del poder aéreo. No obstante, hay dos hechos que siguen siendo incuestionables: debemos mantener y controlar el aire, y el legado de las campañas aéreas en Libia persistirá durante cierto tiempo.⁸¹

Conclusión

Nadie se atrevería a afirmar que no habrá más guerras, porque si así fuera entonces el problema se habría resuelto para siempre; y si tiene que haber guerras se perderán y se ganarán en el aire.

—General de Brigada P. R. C. Groves, Real Fuerza Aérea, 1922

Después de una campaña breve como Odissea del Amanecer/Protector Unificado, probablemente seguirían muchos informes a medida que se dispuso de más información. Esta crítica de ninguna manera desprecia ni disminuye la acción en Libia. Desde un punto de vista retrospectivo, tal vez debamos aceptar la evaluación del Coronel Mark Desens, comandante de la 26 Unidad Expedicionaria Marina: “A pesar de las verrugas . . . y usted y yo sabemos donde estaban esas verrugas . . . tuvo más o menos éxito . . . y ciertamente alivió mucho sufrimiento humano”.⁸² No cabe duda de que sin la intervención, Gadafi habría permanecido en el poder, y sus fuerzas habrían reprimido brutalmente las insurgencias de los rebeldes en Bengasi y todo el país. Por último, la historia juzgará la rectitud y el éxito de la intervención.

A pesar del éxito del resultado, si Estados Unidos y los miembros europeos de la OTAN desean seguir relacionándose para intervenciones similares en el futuro, deben examinar seriamente las deficiencias de esta campaña e incorporar sus lecciones a operaciones futuras. EE.UU. debe examinar la estructura de sus mandos combatientes geográficos, refinar sus procesos de despliegue, hacer compatible o normalizar sus tecnologías, y dejar a las naciones socias asumir el liderazgo en ejercicios combinados. La OTAN tiene obstáculos más difíciles a los que superarse pero, al menos, debe empezar con una decisión estratégica por parte de sus miembros para determinar su compromiso de llevar a cabo operaciones fuera del área. Esta determinación se concentrará en el desarrollo de capacidades durante un período de decrecimiento económico y permitir a los aliados tomar decisiones informadas sobre cómo maximizar la interoperabilidad con la organización. Incluso sin una resolución clara de algunos de las eternas y recurrentes preguntas relacionadas con el poder aéreo, las personas a ambos lados del debate deben seguir considerando con cuidado cómo la campaña conformará enfrentamientos futuros y forzar decisiones estructurales. El siguiente conflicto diferirá de este, así como la operación libia fue diferente de su predecesora. Sin embargo, en vez de reconocer simplemente las deficiencias de Odissea del Amanecer/Protector Unificado, Estados Unidos y la OTAN deben seguir el consejo de Sir John Slessor y aprender de sus experiencias. □

Notas

1. “Last Air Mission of Unified Protector Concluded” (Concluyó la última misión aérea de Protector Unificado), Organización del Tratado del Atlántico Norte, 31 de octubre de 2011, http://www.nato.int/cps/en/natolive/news_80133.htm.

2. Robert Marquand, “NATO Operation in Libya Ends after 7 Months, Could It Be a Model?” (La operación de la OTAN en Libia terminó después de 7 meses, ¿podría ser un modelo), *Christian Science Monitor*, 31 de octubre de 2011, <http://www.csmonitor.com/World/Global-News/2011/1031/NATO-operation-in-Libya-ends-after-7-months-could-it-be-a-model>.

3. Jon Hilsenrath, “Gates Says Libya Not Vital National Interest” (Gates dice que Libia no es de interés nacional vital), *Wall Street Journal*, 27 de marzo de 2011, <http://online.wsj.com/article/SB10001424052748704308904576226704261420430.html>.

4. Análisis de Operaciones Conjuntas y de la Coalición, *Libia: Operation Odyssey Dawn (OOD): A Case Study in Command and Control (Libia: Operación Odissea del Amanecer: caso práctico de comando y control)* (Suffolk, VA: JCOA, 4 de octubre de 2011), 2. (De ahora en adelante Análisis de Operaciones Conjuntas y de la Coalición, *Operación Odissea del Amanecer: caso práctico*).

5. General de División Margaret H. Woodward, “Defending America’s Vital National Interests in Africa” (Defensa de los intereses nacionales vitales en EE.UU.) (discurso, Congreso y Exposición de Tecnología del Aire y del Espacio de la Asociación de la Fuerza Aérea de 2011, National Harbor, MD, 21 de septiembre de 2011), <http://www.af.mil/information/speeches/speech.asp?id=671>.

6. Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: A Case Study (Operación Odisea del Amanecer: caso práctico)*, 9.
7. Análisis de Operaciones Conjuntas y de la Coalición, *Libya: Operation Odyssey Dawn (OOD): Executive Summary (Libia: Operación Odisea del Amanecer: resumen ejecutivo)* (Suffolk, VA: JCOA, 21 de septiembre de 2011), 4. (De aquí en adelante Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: Executive Summary (Operación Odisea del Amanecer: resumen ejecutivo)*).
8. *Ibid.*, 7.
9. *Ibid.*
10. Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: A Case Study (Operación Odisea del Amanecer: caso práctico)*, 8.
11. Análisis de Operaciones Conjuntas y de la Coalición, *Operación Odisea del Amanecer: resumen ejecutivo*, 5; e Instrucción de la Fuerza Aérea 10-401, *Planificación y Ejecución de las Operaciones de la Fuerza Aérea*, 7 de diciembre de 2006, 19, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-401/afi10-401.pdf.
12. Woodward, “Defending America’s Vital National Interests” (Defensa de los intereses nacionales vitales de EE. UU.).
13. *Ibid.*
14. John A. Tirpak, “Lessons from Libya” (Lecciones de Libia), *Air Force Magazine (Revista de la Fuerza Aérea)* 94, no. 12 (diciembre de 2011): 36, <http://www.airforce-magazine.com/MagazineArchive/Documents/2011/December%202011/1211libya.pdf>.
15. Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: A Case Study (Operación Odisea del Amanecer: resumen ejecutivo)*, 5.
16. Inicialmente todos los aviones cisterna y haberes de ISR pesados se enviaron a la Base Aérea de Morón y a la Estación Aérea Naval de Rota, España. Solamente más tarde algunos de los aviones cisterna empezaron a fluir a Istres, Francia. Los aviones de JSTARS y AWACS se trasladaron últimamente a Souda, Grecia, después de un esfuerzo de planificación deliberado. La decisión inicial de enviar AWACS/JSTARS y su gran equipo de mantenimiento/apoyo a Rota significó que en unas cuantas ocasiones durante Odisea del Amanecer, no pudieron volar debido a una cantidad de combustible insuficiente. La mudanza subsiguiente de todos los elementos de apoyo para estos aviones también creó demoras para obtener un transporte aéreo limitado que los estableciera en otra base. Además, la Estación Aérea Naval Sigonella, Italia, ofrece una pista de aterrizaje adecuada para aviones cisterna, pero el avión máximo en el terreno se convirtió en un problema debido a la decisión de establecer en esa base todos los aviones caza. Que sepa, no hubo tampoco un esfuerzo concertado, incluso después de que empezara Protector Unificado, de utilizar algunas de las bases de operación de vanguardia de la OTAN como Aktion, Grecia, y Trapani, Italia, para haberes de EE.UU.
17. El establecimiento de objetivos dinámicos trata de conseguir objetivos de oportunidad que se hayan identificado demasiado tarde o no se hayan seleccionado para entrar en acción a tiempo para la inclusión en objetivos deliberados pero, cuando se detectan o localizan, cumplen criterios específicos para lograr los objetivos. Joint Publication (Publicación Conjunta) (JP) 3-60, *Joint Targeting (Establecimiento conjunto de objetivos)*, 13 de abril de 2007, viii, https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf. La coordinación y el reconocimiento de ataque es una misión volada con el fin de detectar objetivos y coordinar o realizar tareas de ataque o reconocimiento en dichos objetivos. Estas misiones, voladas en un área geográfica específica, son un elemento de la interfaz C2 para coordinar vuelos de interdicción aérea múltiples, detectan y atacan, neutralizan defensas aéreas enemigas y evalúan los daños de las batallas. JP 3-03, *Joint Interdiction (Interdicción conjunta)*, 14 de octubre de 2011, II-14, http://www.dtic.mil/doctrine/new_pubs/jp3_03.pdf.
18. En la experiencia del autor, solo se produjo una órbita de AWACS de 2 horas durante Odisea del Amanecer/ Protector Unificado. Estados Unidos, Reino Unido, Francia y la OTAN volaron cada uno una línea por día. JSTARS voló cada dos días con los aviones de Reconocimiento a Distancia Segura (ASTOR) del Reino Unido en días alternativos pero sin proporcionar una cobertura de 24 horas.
19. El Teniente Coronel Michael W. Lamb Sr., *Operation Allied Force: Golden Nuggets for Future Campaigns (Operación Fuerza Aliada: pepitas de oro para futuras campañas)*, Documento de Maxwell no. 27 (Base de la Fuerza Aérea Maxwell, AL: Air University Press, agosto de 2002), 1–2, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA407618&Location=U2&doc=GetTRDoc.pdf>.
20. Tirpak, “Lessons from Libya” (Lecciones de Libia) 38.
21. Análisis de Operaciones Conjunto y de la Coalición, *Operation Odyssey Dawn: Executive Summary (Operación Odisea del Amanecer: resumen ejecutivo)*, 19.
22. Análisis de Operaciones Conjunto y de la Coalición, *Operation Odyssey Dawn: A Case Study (Operación Odisea del Amanecer: caso práctico)*, 11. Vea también Congreso de EE.UU., Oficina de Evaluación de Tecnología, *New Technology for NATO: Implementing Follow-On Force Attack (Nueva tecnología para la OTAN: implementación del ataque de las fuerzas de seguimiento)* (Washington, DC: Oficina de Impresión del Gobierno, junio de 1987), 118, <http://www.fas.org/ota/reports/8718.pdf>.
23. La observación y las conversaciones personales con oficiales de enlace E-3A de la OTAN. Resaltado también en Myron Hura y otros, *Interoperability: A Continuing Challenge in Coalition Air Operations (Interoperabilidad: un reto continuo en las operaciones aéreas de la coalición)* (Santa Monica, CA: RAND Corporation, 2000), 83, 85, 93, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1235/MR1235.pref.pdf.
24. Tirpak, “Lessons from Libya” (Lecciones de Libia), 35.

25. Orientación, Andrew Shelton, analista de lecciones aprendidas, Tercera Fuerza Aérea / A9, tema: Operación Odisea del Amanecer: la perspectiva de la USAFE, 25 de octubre de 2011.

26. Richard F. Grimmert, *War Powers Resolution: Presidential Compliance (Resolución de potencias bélicas; cumplimiento presidencial)*, Informe CRS para el Congreso RL33532 (Washington, DC: Servicio de Investigación del Congreso, 25 de septiembre de 2012), i, <http://www.fas.org/sgp/crs/natsec/RL33532.pdf>.

27. Tirpak, "Lessons from Libya" (Lecciones de Libia), 35.

28. Ibid.

29. Richard F. Bird y Don Kallgren, "Extending the Mission: NATO AEW beyond Line-of-Sight Airborne IP Communications" (Prolongación de la misión: más allá de las comunicaciones IP aéreas de línea de mira de AEW de la OTAN), Organización del Tratado del Atlántico Norte, septiembre de 2010, <http://www.nc3a.nato.int/SiteCollectionDocuments/MP-IST-092-13.pdf>.

30. Rita Boland, "Building Bridges between Allies, Old and New (Tender puentes entre aliados, antiguos y nuevos)", *SIGNAL Magazine (Revista SIGNAL)*, septiembre de 2010, <http://www.afcea.org/content/?q=node/2382>.

31. Bill Sweetman, "Reluctant Warriors: Fighter Conference Reviews Lessons from Libya Campaign" (Guerreros reacios: congreso de combatientes revisa las lecciones de la campaña de Libia), *Defense Technology International* 5, no. 11 (diciembre de 2011): 19–20.

32. Hura y otros, *Interoperability (Interoperabilidad)*, iii.

33. Amy McCullough, "Libya Mission" (Misión de Libia), *Air Force Magazine (Revista de la Fuerza Aérea)* 94, no. 8 (agosto de 2011): 30, <http://www.airforce-magazine.com/MagazineArchive/Documents/2011/August%202011/0811mission.pdf>.

34. Isabelle François, "NATO and the Arab Spring" (La OTAN y la Primavera árabe), *Transatlantic Current*, octubre de 2011, <http://www.ndu.edu/inss/docUploaded/Transatlantic%20Current%201.pdf>.

35. Julian E. Barnes y Adam Entous, "NATO Air Strategy Gains Renewed Praise" (Se vuelve a elogiar la estrategia aérea de la OTAN), *Wall Street Journal*, 21 de octubre de 2011, <http://online.wsj.com/article/SB10001424052970203752604576643531745513712.html>.

36. Steven Erlanger, "Libya's Dark Lesson for NATO" (La lección siniestra de Libia para la OTAN), *New York Times*, 3 de septiembre de 2011, <http://www.nytimes.com/2011/09/04/sunday-review/what-libyas-lessons-mean-for-nato.html?pagewanted=all>.

37. John Barry, "Lessons of Libya for Future Western Military Forays" (Lecciones de Libia para futuras incursiones militares occidentales), Instituto Europeo, agosto de 2011, <http://www.europeaninstitute.org/EA-August-2011/lessons-of-libya-for-future-western-military-forays.html>.

38. Thom Shanker, "Defense Secretary Warns NATO of 'Dim' Future" (El Secretario de Defensa advierte a la OTAN de un futuro sombrío), *New York Times*, 10 de junio de 2011, <http://www.nytimes.com/2011/06/11/world/europe/11gates.html>.

39. Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: Executive Summary (Operación Odisea del Amanecer: resumen ejecutivo)*, 18.

40. Es difícil encontrar una fuente definitiva y datos debido a las variaciones en lo que las fuentes cuentan como salidas (es decir, salidas, estructuras de aviones y horas). Las fuentes difieren en un 70 a un 85 por ciento. Vea Barry, "Lessons of Libya" (Lecciones de Libia).

41. Ben Barry, "Libya's Lessons" (Lecciones de Libia), *International Institute for Strategic Studies, Survival: Global Politics and Strategy (Instituto Internacional de Estudios Estratégicos, Supervivencia: política y estrategia globales)* 53, no. 5 (octubre–noviembre de 2011): 11.

42. Francis Tusa, "Libya Reveals NATO Readiness Highs and Lows" (Libia pone al descubierto los puntos positivos y negativos del grado de preparación de la OTAN), *Military.com*, 2 de diciembre de 2011, <http://www.military.com/features/0,15240,239146,00.html>.

43. Karen DeYoung y Greg Jaffe, "NATO Runs Short on Some Munitions in Libya" (A la OTAN se le agotan ciertas municiones en Libia), *Washington Post*, 15 de abril de 2011,

44. Michael Clarke y otros, *Accidental Heroes: Britain, France and the Libya Operation (Héroes imprevistos: Gran Bretaña, Francia y la Operación de Libia)* (Londres: Royal United Services Institute (Instituto Real de Servicios Unidos), septiembre de 2011), 6, <http://www.rusi.org/downloads/assets/RUSIInterimLibyaReport.pdf>.

45. Ken Gude y John Podesta, "Libya's Lessons for NATO's Europeans" (Lecciones de Libia para los europeos de la OTAN), *Europe's World*, Primavera de 2012, http://www.europesworld.org/NewEnglish/Home_old/Article/tabid/191/ArticleType/ArticleView/ArticleID/21945/language/en-US/Default.aspx.

46. Lamb, *Operación Fuerza Aliada*, 1–2.

47. Barry, "Libya's Lessons" (Lecciones de Libia) 11.

48. Andrew Tilghman, "U.S. Official: NATO Military Capability Ebbing" (Oficial de EE.UU.: la capacidad militar menguante de la OTAN), *AirForceTimes.com*, 2 de diciembre de 2011, <http://www.airforcetimes.com/news/2011/12/military-nato-military-capability-ebbing-120211w/>.

49. Jim Garamone, "NATO Makes Smooth Transition in Libya Operations" (La OTAN hace una transición sin problemas en las operaciones de Libia), American Forces Press Service, 6 de abril de 2011, <http://www.af.mil/news/story>

.asp?id=123250401; y Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: Executive Summary (Operación Odisea del Amanecer: resumen ejecutivo)*, 19.

50. McCullough, “Libya Mission” (Misión de Libia), 32.

51. Tácticas, técnicas y procedimientos de la Fuerza Aérea 3-3.AOC, *Operational Employment—Air and Space Operations Center (Empleo de las operaciones-Centro de Operaciones Aéreas y Espaciales)* (U), 1 de noviembre de 2007.

52. Análisis de Operaciones Conjuntas y de la Coalición, *Operation Odyssey Dawn: Executive Summary (Operación Odisea del Amanecer: resumen ejecutivo)*, 17.

53. Dave Ehredt, “Command and Control—Exploring Alternatives: The Realities of Two C2 Models for Air Power Proponents” (Comando y control-Exploración de alternativas: las realidades de los dos modelos C2 para proponentes del poder aéreo), *Journal of the JAPCC [Joint Air Power Competence Centre]*, no. 14 (Otoño de 2011): 40, http://www.japcc.de/fileadmin/user_upload/journal/Edition_14/20111014_-_Journal_Ed-14_web.pdf.

54. Análisis de Operaciones Conjuntas y de la Coalición, *Operación Operation Odyssey Dawn: Executive Summary (Odisea del Amanecer: resumen ejecutivo)*, 18.

55. Paul Smyth, “Libya: Is NATO Doing Enough?” (Libia: ¿está haciendo lo suficiente la OTAN), Royal United Services Institute (Instituto Real de Servicios Unidos), 15 de abril de 2011, <http://www.rusi.org/go.php?structureID=commentary&ref=C4DA85C7E0FB14>.

56. Kori Schake, “Lessons of the Libya War” (Lecciones de la guerra de Libia), *Definición de ideas*, 13 de octubre de 2011, <http://www.hoover.org/publications/defining-ideas/article/96531>.

57. François, “NATO and the Arab Spring” (La OTAN y la Primavera árabe), 4.

58. McCullough, “Libya Mission” (Misión de Libia), 30. Vea también Ivo H. Daalder y James G. Stavridis, “NATO’s Success in Libya” (El éxito de la OTAN en Libia), *New York Times*, 30 de octubre de 2011, http://www.nytimes.com/2011/10/31/opinion/31iht-eddaalder31.html?_r=1&adxnnl=1&adxnnlx=1351857791-jUaeHRA3HDly3sD0E5iD+Q&.

59. Richard de Silva, “Lessons from Libya: Gaddafi’s Tactics—and NATO’s Response” (Lecciones de Libia: tácticas de Gaddafi y la respuesta de la OTAN), *Defence IQ*, 25 de octubre de 2011, <http://www.defenceiq.com/air-forces-and-military-aircraft/articles/nato-air-power-lessons-from-libya/>. Teniente General Friedrich Wilhelm Ploeger, vicecomandante del Mando Aéreo Aliado de la OTAN—Ramstein, mencionó en esta entrevista que “[Protector Unificado] llevó a la luz la importancia de los posibilitadores”.

60. Lamb, “Operation Allied Force” (Operación Fuerza Aliada), 38.

61. Dan De Luce y Laurent Thomet, “After Libya, US Cannot Bail Out NATO Shortfalls: Panetta” (Después de Libia, EE.UU. no puede rescatar los déficits de la OTAN: Panetta), Google News, 5 de octubre de 2011, <http://www.google.com/hostednews/afp/article/ALeqM5h1gfsyvWIWoK3EC-XPtS-W-StYCAQ?docId=CNG.7637463e3ae1f3d504fb4d19a47f89ae.151>.

62. W. Bruce Weinrod y Charles L. Barry, *NATO Command Structure: Considerations for the Future (Estructura de mando de la OTAN: consideraciones para el futuro)*, (Washington, DC: Center for Technology and National Security Policy, National Defense University, (Centro de Tecnología y Políticas de Seguridad Nacional, Universidad Nacional de Defensa), 2010), 8.

63. División de Diplomacia Pública de la OTAN, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization (Enfrentamiento activo: concepto estratégico de la defensa y seguridad de los miembros de la Organización del Tratado del Atlántico Norte)* (Bruselas: División de Diplomacia de la OTAN, 19–20 de noviembre de 2010), http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

64. Se trata de valores de nociones usados aquí para describir cómo podrían predefinirse y estar disponibles para planificadores. Las reglas específicas de enfrentamiento o advertencias que una nación pueda tener, ayudan a determinar si alguien podría efectuar el servicio de un objetivo. Una estimación de daños colaterales equivale al nivel del riesgo que alguien desea correr con la posibilidad de daños inintencionados o imprevistos a personas u objetos que no son el objetivo intencionado. Esto afecta y es informado por el tipo de arma que pueda emplearse. Tener información inmediatamente disponible es clave para la interdicción rápida de amenazas, particularmente en un entorno operacional de objetivos dinámicos/coordinación y reconocimiento de ataques.

65. Barry, “Libya’s Lessons” (Lecciones de Libia), 11.

66. Lee T. Wight, “Airpower Dollars and Sense: Rethinking the Relative Costs of Combat” (El dinero y sentido común del poder aéreo: reflexión sobre los costos de combate relativos), *Joint Force Quarterly* 66 (tercer trimestre de 2012): 54–61, <http://www.ndu.edu/press/airpower-dollars.html>; Patrick Cockburn, “NATO in Libya Has Failed to Learn Costly Lessons of Afghanistan” (La OTAN en Libia no ha aprendido las lecciones costosas de Afganistán), *Independent*, 24 de julio de 2011, <http://www.independent.co.uk/voices/commentators/patrick-cockburn-nato-in-libya-has-failed-to-learn-costly-lessons-of-afghanistan-2319539.html>; y Adam J. Hebert, “Libya: Victory through Airpower” (Libia: victoria mediante el poder aéreo), *Air Force Magazine (Revista de la Fuerza Aérea)* 94, no. 12 (diciembre de 2011): 4, <http://www.airforce-magazine.com/MagazineArchive/Documents/2011/December%202011/1211edit.pdf>.

67. Charlie Savage y Mark Landler, “White House Defends Continuing U.S. Role in Libya Operation” (La Casa Blanca defiende el papel continuado de EE.UU. en la operación de Libia), *New York Times*, 15 de junio de 2011, http://www.nytimes.com/2011/06/16/us/politics/16powers.html?pagewanted=all&_r=0; Moni Basu, “Can Air Power End Libya War?” (¿Puede el poder aéreo terminar la guerra de Libia?), CNN.com, 30 de junio de 2011, <http://globalpublic>

square.blogs.cnn.com/2011/06/30/can-air-power-end-libya-war/; George Friedman, "The Emerging Doctrine of the United States" (La doctrina emergente de Estados Unidos), Stratfor, 9 de octubre de 2012, <http://www.stratfor.com/weekly/emerging-doctrine-united-states>; y Carlos Munoz, "Abrial: NATO Closing ISR, Intel Sharing Gaps Exposed in Libya" (Abrial: la OTAN cierra los huecos de ISR, inteligencia al descubierto en Libia), *AOL Defense*, 22 de noviembre de 2011, <http://defense.aol.com/2011/11/22/abrial-nato-closing-isr-intel-sharing-gaps-exposed-in-libya/>.

68. Schake, "Lessons of the Libya War" (Lecciones de la guerra de Libia).

69. Ibid.

70. Robert Farley, "Over the Horizon: Drawing the Right Lessons on Airpower from Libya" (En el horizonte: sacar las lecciones adecuadas del poder aéreo de Libia), *World Politics Review*, 26 de octubre de 2011, <http://web.ebscohost.com/ehost/detail?sid=dc5a6b4f-43f0-44d7-b8cc-eba3929ef1f8%40sessionmgr111&vid=1&hid=107&bdata=JnNpdGU9ZWhvc3QtG12ZQ%3d%3d#db=aph&AN=79973373>.

71. Mayor Jody L. Blanchfield, USAF, *Bombs Away: A Strategic Analysis of Airpower in Limited Conflict (Bombas fuera: un análisis estratégico del poder aéreo en un conflicto limitado)* (Fort Leavenworth, KS: School of Advanced Military Studies, US Army Command and General Staff College, 12 de mayo de 2000), 34, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA381825>.

72. Farley, "Over the Horizon" (En el horizonte).

73. Charles A. Horner, "Air Power Could Be Enough in Libya" (El poder aéreo podría ser suficiente en Libia), *Wall Street Journal*, 24 de marzo de 2011, <http://online.wsj.com/article/SB10001424052748704050204576218813676422854.html>.

74. "Early Military Lessons from Libya" (Primeras lecciones militares de Libia), *IISS* [International Institute for Strategic Studies] (Instituto Internacional de Estudios Estratégicos), *Strategic Comments* 17, comentario no. 34 (septiembre de 2011): 1-3, <http://www.iiss.org/publications/strategic-comments/past-issues/volume-17-2011/september/libya-early-military-lessons/>.

75. Ibid.

76. Dr. Christian F. Anrig, "Allied Air Power over Libya: A Preliminary Assessment" (El poder aéreo aliado en Libia: evaluación preliminar), *Air and Space Power Journal* 25, no. 4 (Invierno de 2011): 104, http://www.airpower.au.af.mil/airchronicles/apj/2011/2011-4/2011_4.pdf.

77. Documento de Doctrina de la Fuerza Aérea 1, *Air Force Basic Doctrine, Organization, and Command (Doctrina, organización y comando básicos de la Fuerza Aérea)*, 14 de octubre de 2011, 16, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf>.

78. Ibid., 129.

79. Farley, "Over the Horizon" (En el horizonte).

80. Ibid.

81. Trish Turner, "McCain Calls for Air Strikes against Syria's Assad" (McCain pide ataques aéreos contra Assad de Siria), *Fox News*, 5 de marzo de 2012, <http://www.foxnews.com/politics/2012/03/05/mccain-calls-for-air-strikes-against-syrias-assad/>.

82. Coronel Mark Desens, comandante de la 26 Unidad Expedicionaria Marina durante Odisea del Amanecer, entrevista por el autor, 7 de diciembre de 2011.



El Mayor Jason R. Greenleaf, USAF (USAFA; MBA, Trident University International; MMS, Marine Corp University) se desempeña en la actualidad como oficial en la división de operaciones en la Dirección de Gestión de Recopilación de Información, Agencia de Inteligencia de la Defensa. El Mayor Greenleaf ayuda en la dirección y administración del personal conjunto militar y civil de la división, administra los requerimientos de recopilación permanentes, en los que el factor tiempo es importante y en caso de crisis. Un piloto experto con más de 2.750 horas de vuelo en el C-21A y el E-3B/C, anteriormente se desempeñó en calidad de piloto evaluador oficial en una unidad de entrenamiento y jefe de Grupo de Operaciones de Estandarización y Evaluación en la Base Aérea Tinker, Oklahoma. El Mayor Greenleaf es egresado de la Escuela Superior para Oficiales de Escuadrón y de la Escuela Superior de Comando y Estado Mayor del Cuerpo de Infantería de Marina.

Funciones de Inteligencia, Vigilancia y Reconocimiento en Vuelo con Operadores Humanos

¿Estratégicas, Tácticas . . . las dos Cosas?

MAYOR TYLER MORTON, USAF

Nos hemos adaptado a los tiempos . . . desde ser un haber predominantemente estratégico que puede aplicar una cantidad tremenda de capacidad en el entorno táctico.

—Teniente Coronel Rich Rosa,
Comandante Escuadrón de reconocimiento expedicionario 763, 2011

EL DESEO DEL gobierno de Obama de reequilibrar el enfoque global de Estados Unidos en las regiones del Pacífico Occidental y de Asia Oriental tiene serias ramificaciones para la comunidad de inteligencia, vigilancia y reconocimiento (ISR) en vuelo con operadores humanos.¹ Dicha fuerza, históricamente versada en recopilación de inteligencia a nivel estratégico, se ha convertido—debido a las exigencias de los conflictos de la contrainsurgencia de principios del siglo XXI—en el primer proveedor mundial de inteligencia a nivel táctico. El arsenal de haberes de ISR en vuelo con operadores humanos de la Fuerza Aérea de EE.UU. es una institución en los campos de batalla de Afganistán, y los combatientes terrestres se basan en estas plataformas para la inteligencia táctica.² La inteligencia que la fuerza de ISR en vuelo con operadores humanos de Estados Unidos comunica significa a menudo la diferencia entre la vida y la muerte de las fuerzas terrestres enfrentadas en combate. Sin embargo, no fue siempre así. Antes de la Guerra del Golfo Pérsico, estas plataformas dominaban el programa de reconocimiento aéreo en tiempos de paz. Pasaron la Guerra Fría volando cerca de la periferia de la Unión Soviética—y de muchas otras naciones—recopilando inteligencia diseñada para informar a los encargados de tomar decisiones a nivel nacional. La ISR en vuelo con operadores humanos se transformó a partir de la Guerra del Golfo Pérsico y se desarrolló por completo en la Operación Libertad Duradera. La nueva fuerza, primero dando indicaciones y advirtiendo a las tripulaciones aéreas que patrullaban Irak y desarrollando la capacidad de advertir de las amenazas en tiempo casi real a las fuerzas terrestres de Afganistán, es ahora un proveedor de inteligencia táctica de clase mundial. No obstante, el futuro reequilibrio de Asia y la casi simultánea reducción de tropas en Afganistán anuncian un cambio en la misión. La pregunta es ahora, ¿qué va a ocurrir a continuación al ISR en vuelo con operadores humanos?

Si se produce un cambio de misión para la ISR en vuelo con operadores humanos, la fuerza requerirá cambios fundamentales de su capacidad. Una comunidad que ahora depende en gran medida de la misión de soporte táctico necesita tiempo para reorientarse a una mentalidad estratégica. Dos décadas de vuelos en Irak y Afganistán sin duda han mermado la capacidad de la comunidad de llevar a cabo misiones sostenidas en el teatro de operaciones del Pacífico; la mayoría de los aviadores que volarán estas misiones se educaron en el entorno táctico. Además, la comunidad de ISR en vuelo con operadores humanos se enfrenta a la posibilidad de mantener ambas capacidades—estratégica y táctica. Como indica la siguiente explicación, a las fuerzas de ISR en vuelo con operadores humanos se les ha pedido históricamente que fluctuaran entre recopilar inteligencia estratégica y táctica. No obstante, tradicionalmente, al final de la termina-

ción del requisito táctico (Corea, Vietnam), la fuerza de ISR volvió a su enfoque estratégico. ¿Será diferente esta vez? ¿Tratará la Fuerza Aérea de mantener cierto nivel de capacidad de soporte táctico o lo abandonará, como lo ha hecho muchas otras veces? Si decide retener una capacidad táctica, se enfrenta al reto inenvidiable de adiestrar y mantener una recopilación, un procesamiento y una explotación diferentes; análisis y producción; y tácticas, técnicas y procedimientos de diseminación.

Por último, la Fuerza Aérea también se enfrenta a la tarea intimidadora de conservar la flota de ISR en vuelo con operadores humanos en tiempos de austeridad fiscal. Según se ha resaltado en la explicación subsiguiente, después de períodos importantes de combate, Estados Unidos tradicionalmente ha tratado de disminuir la fuerza; las fuerzas de ISR no han sido siempre inmunes a estos cortes. Afortunadamente, la historia ofrece muchos ejemplos de cambios en la misión de ISR en vuelo con operadores humanos y su capacidad de perseverar, a pesar a veces de las restricciones de presupuesto draconianas. Desde el establecimiento de unas funciones de ISR estratégicas uniformes en vuelo con operadores humanos contra la Unión de Repúblicas Socialistas Soviéticas (URSS) hasta la misión táctica de hoy en Afganistán, se ha pedido a la fuerza de ISR en vuelo con operadores humanos que altere su dirección muchas veces. Al examinar el desarrollo inicial de dicha fuerza y hacer el seguimiento de sus cambios de misión históricos, este artículo muestra que las fuerzas de ISR en vuelo con operadores humanos se han adaptado antes y pueden volver a hacerlo nuevamente. Los factores limitadores—tanto ahora como en el pasado—incluyen tiempo, personal y recursos.

Funciones de ISR estratégicas en vuelo con operadores humanos

Aunque las fuerzas militares se imaginaron y operaron primero un ISR en vuelo con operadores humanos como un haber de recopilación táctica, la incapacidad de los globos y aviones de proporcionar una inteligencia oportuna de forma rápida y coherente a los clientes de tierra condujo a las fuerzas de todo el mundo a empezar a usar sus plataformas áreas para suministrar una inteligencia estratégica. Al principio de la PGM, los comandantes terrestres creyeron que el reconocimiento aéreo del frente y la observación de artillería eran la contribución principal de la aviación a la guerra terrestre. Ambas misiones vinculaban inextricablemente la aviación—globos o aviones—con el combatiente terrestre. A pesar de la vinculación, al empezar la guerra, los ejércitos siguieron sin estar seguros del valor de la nueva capacidad. Las comunicaciones siguieron siendo problemáticas, y muchos comandantes terrestres escépticos siguen cuestionando la veracidad de la inteligencia obtenida por observación.³ Además, una serie de observadores en vuelo exageraron sus informes.⁴ No obstante, a medida que se produjo un estancamiento en el terreno, las funciones de ISR en vuelo se convirtieron en el medio principal—aunque no en el único—de recopilar inteligencia acerca de los movimientos del enemigo. El desarrollo técnico de la aviación y las capacidades adicionales que ofrecieron también justificaban la nueva confianza en ISR.

El avance de la aviación fue muy rápido—nuevas plataformas alcanzaron el frente, para verse en desventaja en cuestión de meses por el desarrollo siguiente.⁵ Durante el curso de la guerra, las velocidades en el aire se duplicaron, las altitudes máximas y las velocidades de ascenso se triplicaron, la potencia del motor aumentó cinco veces y los aviones añadieron armamento.⁶ Estos aumentos de capacidades fueron acompañados por tareas adicionales. A finales de la guerra, los aviones estaban volando un gran número de misiones, muchas de ellas nuevas: bombardeo estratégico, interdicción aérea, ataque desde portaaviones, defensa aérea, ataques terrestres e ISR.

Las funciones de ISR no eran nuevas, pero la profundidad y altura a la que los aviones podían penetrar en el territorio enemigo habían cambiado. Las capacidades adicionales permitían unas funciones de ISR de penetración profunda y alteraron fundamentalmente el tipo de inteligencia suministrado por la aviación. Las funciones de ISR en vuelo ya no se limitaban a las líneas del

frente, ni tampoco estaba ligado a los combatientes de tierra; las nuevas capacidades permitieron a los aviones ver en el interior del territorio enemigo y los aviadores pudieron predecir el curso de acción de un enemigo. Al ver los movimientos del enemigo muy por detrás de las líneas del frente, los aviadores de ISR podían pronosticar sus intenciones con tiempo suficiente para que las fuerzas amigas repelieran los asaltos y frustraran sus planes. Debido a estas nuevas capacidades, los aviadores validaron rápidamente su significado.

En la Primera Batalla del Marne, las funciones de ISR en vuelo de gran penetración detectaron un error fatal cometido por el General Alexander von Kluck de Alemania. En un movimiento diseñado para cortar el acceso a París de las fuerzas francesas principales, von Kluck dirigió sus unidades al este. Al hacer esto, expuso todo el flanco derecho del Primer y Segundo Ejércitos alemanes.⁷ Los haberes de ISR en vuelo con operadores humanos detectaron la debilidad, permitiendo a dos ejércitos franceses y a la Fuerza Expedicionaria Británica aprovecharse de ellos y derrotar a los alemanes, forzándoles a retirarse a 65 kilómetros hasta el río Aisne, donde empezaron a fortificar sus posiciones para lo que se convertiría en la infame guerra de las trincheras.⁸ La Primera Batalla del Marne cambió el curso de la guerra. Las funciones de ISR en vuelo con operadores humanos proporcionaron la información de inteligencia que permitía a los comandantes aliados actuar de forma decisiva y salvar lo que parecía una probable derrota francesa y la pérdida de París.

En este ejemplo, los aviones de ISR tenían tiempo suficiente para regresar de sus salidas e informar sobre lo que habían visto, al igual que los franceses y británicos tenían tiempo de diseñar un contraataque. La recopilación estratégica estaba empezando a cobrar forma. No obstante, seguía habiendo problemas en la comunicación directa aire a tierra. La incapacidad de la aviación de enviar información de inteligencia de forma precisa y rápida, ya pronosticada en 1907 por Benjamin Foulois, futuro jefe del Cuerpo Aéreo, fue la ruina de las funciones tácticas de ISR.⁹ Durante las primeras etapas de la guerra, el método principal de comunicar la inteligencia obtenida de las salidas de ISR pedía al piloto aterrizar su avión cerca de la batería de artillería y simplemente indicaba a los artilleros lo que había averiguado.¹⁰ Cuando era posible, los observadores anotaban las ubicaciones de las baterías de artillería hostiles en mapas para completar sus descripciones.¹¹ Estos informes a menudo demostraron ser imprecisos porque en la emoción del primer fragor del combate, el adiestramiento anterior inadecuado de los observadores les conducía frecuentemente a la identificación equivocada de las nacionalidades y actividades de las tropas.¹² El uso de fotografías aéreas ayudó a eliminar algunos de estos problemas, pero la fuerza de ISR en vuelo nunca superó las dificultades con la comunicación táctica. Aunque esta situación selló fundamentalmente el destino de la recopilación de inteligencia táctica del momento, abrió la puerta del nivel estratégico de ISR en vuelo con operadores humanos que tipificaría la mayor parte del esfuerzo de las Fuerzas Aéreas del Ejército de Estados Unidos (USAAF) durante la SGM y después.

El poder aéreo emergió de la PGM como un complemento valioso a las capacidades del Ejército, pero siguió siendo vulnerable a las reducciones importantes de fuerzas y a la vuelta al aislacionismo que caracterizó el período. Aunque la Ley de Defensa Nacional de 1920 reconoció el éxito del poder aéreo estableciendo el Servicio Aéreo como una rama independiente del Ejército, hacia finales de 1920, el Ejército había instituido cortes drásticos en la aviación en un intento de modernizar las fuerzas terrestres.¹³ Los aviadores no habían ascendido a los escalafones más altos de liderazgo del Ejército y por lo tanto no tenían poder para impedir los cortes en aviación pedidos por los Generales terrestres estrechos de miras. Este alejamiento del aire y acercamiento a tierra dejó al Cuerpo Aéreo, particularmente a las incipientes fuerzas de ISR, con poco dinero para adquirir nuevos aviones y con pocas personas para hacer avanzar la doctrina del poder aéreo en la era moderna.

A medida que se desarrollaba una nueva guerra en Europa y el Pacífico, las funciones de ISR en vuelo de EE.UU. se encontraron muy poco preparadas. La doctrina de ISR no había avan-

zado, y aun cuando la PGM había establecido el valor de la recopilación de inteligencia estratégica, las funciones de ISR en vuelo siguieron ligadas, desde el punto de vista de la doctrina, a las fuerzas terrestres e inherentemente tenían un corto alcance por naturaleza. Además de una doctrina estancada, las capacidades de la aviación de ISR no habían mantenido el ritmo con las fuerzas armadas rápidamente modernizadoras. Los aviadores habían abogado enérgicamente por una aviación de reconocimiento adicional, pero cuando empezó la participación de EE.UU. en la guerra, en 1941, el Cuerpo Aéreo poseía pocas estructuras de aviones modernas.¹⁴

Las funciones de ISR en vuelo, a pesar de un entorno que no fomentaba la innovación, estaban al borde de una evolución grande. A medida que avanzaba la SGM, sus mejores capacidades de aviación, junto con una gran determinación, permitieron a las fuerzas de ISR en vuelo de EE.UU. hacer contribuciones significativas al éxito de los aliados. Además de la increíble expansión de la misión de inteligencia de imágenes (IMINT) que habían validado durante la PGM, las fuerzas de ISR en vuelo de la SGM crearon una capacidad de primera clase para recopilar inteligencia de comunicaciones (COMINT) e inteligencia electrónica (ELINT). En el verano de 1942, durante vuelos para determinar la extensión de cobertura de los radares alemanes en las áreas de Cerdeña-Taranto-Tripoli, los británicos experimentaron con la introducción de lingüistas en aviones del escuadrón Wellington ELINT 162.¹⁵ Su capacidad de avisar a los pilotos por adelantado de la actividad de combate alemana se hizo muy valiosa. Como en el caso de muchos otros desarrollos, los estadounidenses adoptaron el procedimiento británico, y en octubre de 1943 volaban con lingüistas en sus aviones mediterráneos de investigación de irradiación electromagnética ELINT.¹⁶ Además de proteger las formaciones de aviones y bombarderos, los lingüistas podían llamar a combatientes amigos para atacar a los aviones alemanes. Según el Teniente Roger Ihle, uno de los primeros oficiales de combate electrónico en vuelo de EE.UU., “Teníamos a estos muchachos que hablaban alemán y que estaban vigilando todas las frecuencias de aviación de los alemanes, de modo que cuando oyeron a los alemanes empezar a hacer despegues de urgencia, comunicaron a los combatientes [estadounidenses] lo que estaba pasando”.¹⁷ La presencia de lingüistas mejoró la situación, por lo que a fines de 1944, las tripulaciones de los bombarderos volaban comúnmente con un número de ellos a bordo.¹⁸

Estos avances—IMINT, COMINT y ELINT mejorados—solidificaron la función de la inteligencia estratégica aérea. De hecho, debido al desarrollo de estas nuevas capacidades, los términos *reconocimiento aéreo estratégico* y *reconocimiento aéreo táctico* habían pasado a formar parte ya del vocabulario de la USAAF antes de que acabara la guerra. En el apéndice de inteligencia del informe de la USAAF sobre las contribuciones del poder aéreo a la derrota de Alemania, las Fuerzas Aéreas de EE.UU. en Europa/A-2 definieron *reconocimiento aéreo estratégico* como “el programa de adquirir inteligencia aérea como base para llevar a cabo una guerra aérea estratégica contra el enemigo” y un *reconocimiento aéreo táctico* como algo que se ocupaba de la “cobertura diaria a gran escala de las áreas avanzadas del enemigo, fotografía de evaluación de daños para ataques de cazabombarderos, y defensas enemigas, campos de aviación y otros objetivos especiales hasta 240 kilómetros del frente”.¹⁹ Además, el estudio de bombardeo estratégico de Estados Unidos concluyó que “EE.UU. debe tener una organización de inteligencia capaz de conocer las vulnerabilidades, capacidades e intenciones estratégicas de cualquier enemigo potencial”.²⁰ Esta descripción clara solidificó las necesidades de la USAAF de una capacidad de recopilación estratégica indígena en vuelo a largo plazo después de la guerra y armó la futura Fuerza Aérea con la justificación de sostener el crecimiento de funciones de ISR en vuelo.

Después de la PGM, las fuerzas militares de EE.UU. experimentaron una reducción importante ya que la vuelta al aislacionismo se había convertido en la nueva filosofía. No obstante, después de la SGM, Estados Unidos se enfrentó a una amenaza que no podía evitar con un simple repliegue. A medida que se intensificó la Guerra Fría con la URSS, se evidenció que los soviéticos serían un adversario importante en el futuro previsible. En una época anterior a los misiles balísticos intercontinentales, los bombarderos de largo alcance de la Fuerza Aérea

representaban la única opción de ataque viable de Estados Unidos. Cuando los planificadores de la Fuerza Aérea empezaron a reunir información de objetivos para la guerra aérea estratégica, reconocieron rápidamente la escasez de inteligencia sobre la URSS. Si se les llamaba, los bombarderos de la Fuerza Aérea necesitaban conocer los objetivos soviéticos críticos; a fines de los años 40, la información derivada de EE.UU. simplemente no existía.²¹ Cuando los soviéticos se incorporaron a la era nuclear en 1949, la necesidad se hizo suprema.

Para satisfacer las demandas de inteligencia de la Guerra Fría, la Fuerza Aérea empezó a llevar a cabo misiones de inteligencia estratégicas en vuelo a lo largo de la periferia del territorio en manos soviéticas. Inicialmente, los aviones de ISR—normalmente, los C-47, B-17 o B-24 modificados—basados en Gran Bretaña y en la Alemania ocupada produjeron mapas fotográficos de grandes áreas bajo control soviético.²² Según un proyecto conocido como “Casey Jones”, los aviones de la Fuerza Aérea fotografiaron más de 5.000.000 de kilómetros cuadrados de Europa y África del Norte.²³ En el Ártico, los B-29 modificados de la primera unidad operacional del Comando Aéreo Estratégico (SAC)—el 46 escuadrón de reconocimiento—hizo fotografías de lugares potenciales de diversión para bombarderos SAC.²⁴ Las IMINT demostraron ser útiles, pero la incapacidad de obtener fotografías de largo alcance, junto con el mayor peligro planteado por las defensas aéreas soviéticas, obligó a los planificadores a buscar otras soluciones. En septiembre de 1946, SAC empezó a volar misiones de recopilación de ELINT especiales junto con potenciales rutas de bombardeo árticas con el fin de caracterizar las posiciones de radar soviéticas.²⁵ Aunque con éxito, las salidas describían solamente una pequeña imagen de las defensas aéreas de la URSS. Para entender verdaderamente la amenaza, Estados Unidos tendría que ordenar vuelos de incursión del territorio soviético.

Frustrado por la falta de información de las ubicaciones de los radares soviéticos y sus capacidades, y con unos datos de mapa imprecisos del litoral soviético, el 5 de abril de 1948, el Secretario de la Fuerza Aérea, Stuart Symington envió una carta al General Carl Spaatz, jefe de estado mayor de la Fuerza Aérea, expresando su preocupación por la falta de detalles e instando a Spaatz a autorizar los vuelos de incursión directos en la URSS.²⁶ Spaatz estuvo de acuerdo, y el 5 de agosto de 1948, el escuadrón de reconocimiento 46 llevó a cabo la primera misión autorizada para sobrevolar la URSS.²⁷ Estas salidas tan exitosas generaron imágenes sin precedentes de posiciones de radar soviéticos así como una fotografía detallada del litoral ruso. No obstante, las defensas aéreas soviéticas evolucionaron rápidamente y a principios de los años 50, cuando el riesgo de perder un avión sobre territorio soviético se hizo demasiado grande, el Presidente Dwight Eisenhower ordenó el desarrollo del U-2. Dicho avión gozó de un éxito temprano al sobrevolar la URSS, pero el incidente de Francis Gary Powers de mayo de 1960 relegó nuevamente la recopilación de inteligencia estratégica aérea a la periferia de la URSS.²⁸

Durante la Guerra Fría, el uso de aviones de ISR para recopilar inteligencia estratégica se convirtió en un requisito clave para entender a las fuerzas armadas soviéticas. Las misiones de sobrevuelo periféricas y directas proporcionaron la inteligencia que Estados Unidos necesitaba estar un paso por delante de los soviéticos. La recopilación de inteligencia estratégica, aunque a menudo peligrosa, no da típicamente una sensación de urgencia.²⁹ Aunque normalmente no es sensible con respecto al tiempo, contribuye a un entendimiento general del enemigo.³⁰ Pero en ocasiones la Fuerza Aérea usó sus plataformas de funciones de ISR estratégicas en vuelo para apoyar a comandantes tácticos directamente. Estas situaciones retaron a la comunidad de ISR porque la información recogida a menudo significaba la vida o la muerte para las tropas en tierra y otros aviadores en los cielos. En Corea y Vietnam, los aviadores de ISR en vuelo desarrollaron formas innovadoras de asegurarse de que su inteligencia alcanzara al combatiente. Sus esfuerzos demostraron que los haberes de ISR en vuelo podían satisfacer ambas funciones—estratégica y táctica—pero la transición completa requirió tiempo e inventiva.

La Guerra de Corea: COMINT a la cabina del piloto

Cuando Corea del Norte invadió el sur en junio de 1950, las funciones de ISR en vuelo de EE.UU. estaban muy mal preparadas para proporcionar a los comandantes terrestres y aéreos el respaldo que necesitaban. La escasez de lingüistas, interpretadores de fotografías, equipos y aviones contribuyeron a la falta de información en las primeras etapas del conflicto. No obstante, a medida que la guerra siguió su curso, las funciones de ISR evolucionaron. Los aviadores del Servicio de Seguridad de la Fuerza Aérea de EE.UU. (USAFSS) crearon un sistema para suministrar COMINT aérea directamente a las cabinas de aviones caza y bombarderos, suministrándoles información de la situación sin precedentes. Estos éxitos en Corea establecieron las bases para la integración de ISR en vuelo en conflictos subsiguientes.

Cuando empezó la guerra, las Fuerzas Aéreas del Lejano Oriente (FEAF) señalaron que la capacidad de inteligencia (SIGINT) estaba en una condición atroz. En junio de 1950, el primer escuadrón de radio móvil de la USAFSS, la única unidad de SIGINT operacional bajo el control de FEAF, no poseía una capacidad de recopilación aérea.³¹ Además, al principio de la guerra, el escuadrón no tenía lingüistas coreanos ni un acceso limitado a COMINT de Corea del Norte.³² En un informe interno, el USAFSS caracterizó a su SIGINT al principio de la guerra como “lastimosamente pequeño y concentrado en lugares equivocados”.³³

Inmediatamente después del estallido de la guerra, los aviadores del USAFSS empezaron a desarrollar formas innovadoras para aportar inteligencia al combatiente. Justo como lo habían hecho en la SGM, los aviadores empezaron a volar como “acompañantes” en aviones que no eran de ISR. Ya a principios de enero de 1951, la Unidad 4 del escuadrón de transporte de tropas 21 volaba misiones de bajo nivel de penetración profunda en territorio norcoreano con el fin de infiltrar espías amigos. Estas salidas de Douglas C-47 llevaban a menudo a un aviador estadounidense de origen coreano a aconsejar a los aviones de la misión sobre la actividad enemiga y apoyar los requisitos de inteligencia de la Quinta Fuerza Aérea.³⁴ Solamente en ese mes, la unidad voló hasta 13 misiones de “intercepción de radio”.³⁵ Estas incursiones dentro de las líneas enemigas ayudaron a entender sin precedentes a FEAF sobre la situación del enemigo y contribuyeron significativamente al esfuerzo de planificación aérea de la quinta Fuerza Aérea.³⁶

En febrero de 1953, el USAFSS, al tratar de mover la inteligencia directamente a la cabina del piloto, instaló una posición de recopilación de COMINT en un centro de control aéreo táctico C-47 en vuelo.³⁷ Al principio, “Mosquito Mellow”, como se llegó a conocer, pasaba mensajes entre partes de control aéreo táctico, controladores en vuelo, cazabombarderos y la estación de control terrestre.³⁸ De todas formas, con el tiempo, la proeza del avión en acortar la cadena de comunicaciones entre la aviación táctica y la estación de control terrestre hizo que se convirtiera en un puesto de mando en vuelo de facto. El USAFSS instaló un método de comunicación seguro que dejaba que el lingüista abordó validara la inteligencia que recopiló con la unidad terrestre del Destacamento 153 del USAFSS. Después de confirmar la información, el lingüista la envió después a la tripulación del centro de control aéreo táctico, que rápidamente la pasó directamente a otro avión del área. Este proceso a menudo tenía el efecto de desviar aviones caza, bombarderos y fuerzas terrestres de sus misiones primarias para apoyar situaciones emergentes a medida que eran detectadas por el lingüista en vuelo.³⁹

El esfuerzo final realizado por el USAFSS para suministrar COMINT en vuelo directamente al combatiente se produjo en un proyecto conocido como Blue Sky. El Mayor Leslie Bolstridge del Grupo de Seguridad 6920 propuso la idea de equipar los C-47 con equipos de recopilación de COMINT.⁴⁰ A fines de 1952, FEAF dio al grupo tres C-47, asignándoles al escuadrón móvil de radio en vuelo 6053 en la Base Aérea de Yokota (AB), Japón.⁴¹ Inmediatamente casi al comienzo, las operaciones fueron un gran éxito. Al sobrevolar la península de Corea y el Mar de Japón, el recientemente dotado RC-47 suministró un acceso sin precedentes a objetivos en el interior de Corea del Norte y China. Aun cuando los C-47 no tenían comunicaciones directas con los com-

batientes, unos aviadores ingeniosos idearon un sistema por el que el avión lanzaría sus grabaciones de cinta magnética a miembros esperando en la unidad terrestre del Destacamento 153 del USAFSS en la Isla Cho Do, Corea. En un procedimiento que presagió el mecanismo de suministro de satélite de imágenes de CORONA, la tripulación del RC-47 adaptó paracaídas a las cintas grabadas y después las lanzó en un área designada de la playa en la isla.⁴² Las cintas pasaron rápidamente al Destacamento 153, que subsiguientemente transmitieron cualquier inteligencia pertinente directamente a los combatientes. Aunque no son tan oportunas como llegó con el tiempo a convertirse la advertencia directa de amenazas, este método proporcionó una inteligencia valiosa. Como prueba de su valor, cuando uno de los RC-47 del escuadrón se estrelló durante un despegue de Yokota AB, el General Otto Weyland, el comandante de FEAF, ofreció su propio VIP C-47 como reemplazo del avión dañado.⁴³

Cuando empezó la guerra, las funciones de ISR en vuelo no tenían capacidad táctica significativa. No obstante, como se había hecho en la SGM, la Fuerza Aérea construyó una fuerza de COMINT en vuelo competente. Abandonadas en su mayor parte en las primeras etapas de la guerra, la COMINT en vuelo se convirtió en un gran contribuyente al éxito del poder terrestre y aéreo. Y lo que es importante, la capacidad de los aviadores de cambiar su enfoque rápidamente de la URSS a Corea no mostró solamente su flexibilidad sino también el poder de la innovación. Cuando están debidamente dotados con equipos adecuados—en este caso el C-47—las tripulaciones aéreas improvisaron y encontraron nuevas formas de contribuir a la lucha. Sus experiencias en Corea ayudaron a los aviadores que les sucedieron a que repitieran muchos de sus logros en la Guerra de Vietnam.

Vietnam: Proyecto Teaball

Las operaciones con éxito de los destacamentos del USAFSS durante la Guerra de Corea hizo posible el suministro de COMINT saneada al combatiente. Doyle Larson, un coronel en esa época, desarrolló quizás el esfuerzo más conocido de la Guerra de Vietnam al desarrollar un sistema similar llamado Proyecto Teaball. Aunque el esfuerzo de la Guerra de Corea proporcionaba solamente COMINT, el sistema de Larson activó la diseminación rápida de la información de múltiples fuentes directamente al combatiente.

Como respuesta a una petición de ayuda del General John Vogt, comandante de la Séptima Fuerza Aérea, el equipo de Larson investigó formas de proteger los aviones de la Séptima.⁴⁴ Debido a que los continuos vuelos de U-2 sobre Laos estaban ya enviando la inteligencia reunida a una furgoneta en la Base de la Fuerza Aérea Real Tailandesa de Nakhon Phanom en Tailandia, el equipo de Larson decidió que la preparación de una furgoneta de mando y control junto a la furgoneta de explotación de U-2 constituía la mejor forma de comunicar la inteligencia.⁴⁵ Este nuevo sistema permitiría a la furgoneta de mando y control pasar información de advertencia sobre amenazas directas a pilotos a los pocos segundos de su recepción.

En las semanas siguientes, tanto el General Vogt como el General John Ryan, jefe de estado mayor de la Fuerza Aérea, aprobaron el proyecto y dirigieron su implementación. Después de llegar al teatro de operaciones y temeroso de basarse únicamente en la recopilación de información de los U-2, los miembros del equipo de Larson empezaron a buscar más plataformas a las que podrían contribuir.⁴⁶ Al visitar las tripulaciones de RC-135M Rivet Card en Japón, descubrieron que el avión pasaría su recopilación al escuadrón de seguridad 6929 del USAFF en Osan, Corea, que podría transmitirse después a la furgoneta Teaball en Nakhon Phanom por medio de comunicaciones seguridad. Además de la información de U-2 y RC-135, también incorporaban datos de EC-121 Warning Star en órbita y barcos piquete equipados con radar de la Armada de EE.UU. Estas múltiples fuentes de información dieron al centro de operaciones de Teaball la imagen de inteligencia más robusta disponible.

El 26 de julio de 1972, entró en vigor el proyecto.⁴⁷ Después de sufrir las dificultades del comienzo marcadas por los problemas de las comunicaciones, el proyecto acabó teniendo un éxito enorme.⁴⁸ Como en Corea, los pilotos de EE.UU. ahora tenían la información necesaria para evitar emboscadas aéreas y tender las suyas. En unas semanas, los pilotos estaban poniéndose en contacto con el Centro de Control de Armas Teaball antes de sus salidas para asegurarse de que pudieran recibir inteligencia derivada de Teaball.⁴⁹ La relación de aniquilamiento aire a aire aumentó de 1:2 (antes de Teaball) a más de 4:1.⁵⁰ Si nos fijamos en las operaciones Teaball, el General Vogt declaró que “con el advenimiento de Teaball, invertimos dramáticamente esto [relación pérdida a victoria]. . . . Durante Linebacker derribábamos al enemigo a un ritmo de cuatro a uno . . . mismo avión, mismo entorno, mismas tácticas; en gran medida [la] diferencia [era] Teaball.”⁵¹

Teaball había demostrado de forma inequívoca que las fuerzas de ISR en vuelo podrían suministrar inteligencia directamente al combatiente. Como era el caso en Corea, la inventiva de los aviadores marcó la diferencia. Dados el tiempo y los recursos, alteraron la mentalidad de la inteligencia estratégica basada en los soviéticos a una altamente capaz de suministrar inteligencia directamente a los que la necesitaban. No todo fue perfecto: las complicaciones de las comunicaciones, la confusión de los lingüistas y el hecho de que hubo que convencer a los pilotos complicaron el sistema, pero al final, la inteligencia suministrada por las fuerzas de ISR en vuelo salvaron vidas.⁵²

Después de Vietnam, las fuerzas de ISR con operadores humanos descartaron nuevamente las lecciones aprendidas de la guerra y volvieron a la recopilación de inteligencia estratégica contra los soviéticos. Esta reorientación en la URSS continuó hasta que la Operación Furia Urgente en Granada destacó nuevamente el suministro de inteligencia táctica a clientes terrestres conjuntos.⁵³ Después, los ingenieros de aviación trabajaron incansablemente para automatizar el flujo de datos y suministrar radios compatibles que permitieran a las tripulaciones hablar directamente con las fuerzas terrestres y otros haberes aéreos. En el momento en que empezaron las Operaciones Escudo del Desierto y Tormenta del Desierto, estas capacidades estaban disponibles. Durante los conflictos de la contrainsurgencia de principios del siglo XXI, las tripulaciones de ISR en vuelo con operadores humanos afinaron estas capacidades de modo que ahora podemos ofrecer advertencia de amenazas e información del enemigo en tiempo casi real a una multitud de combatientes.

Conclusión

Por supuesto, la habilidad táctica de las fuerzas actuales de ISR en vuelo con operadores humanos sigue siendo crítica para la ejecución con éxito de las operaciones terrestres y ha salvado innumerables vidas, pero sin un liderazgo firme, el futuro reequilibrio en el Pacífico podría anunciar la desaparición de dicha suficiencia. El debate anterior ha demostrado que, al volver a sus incursiones de recopilación táctica, las fuerzas de ISR en vuelo con operadores humanos de la Fuerza Aérea han abandonado históricamente su misión de recopilación táctica. No obstante, el futuro desplazamiento a Asia-Pacífico después de la reducción de tropas en Afganistán, difiere de los estudios prácticos aquí mencionados. Al ir a Corea y Vietnam, la Fuerza Aérea tenía que crear nuevas capacidades de aviación y métodos de diseminación para suministrar inteligencia táctica a los combatientes. Este no será el caso al salir de Afganistán. Las fuerzas de ISR en vuelo han integrado estas capacidades tácticas en las referencias de la aviación. Tanto si usamos estas plataformas para recopilar inteligencia táctica como estratégica, seguirán sus radios y avances en la distribución de datos, permitiendo a los haberes volar sin dificultades del entorno táctico al estratégico según sea necesario y tomar la decisión de mantener la aptitud en la recopilación táctica más sencilla. Desertamos la misión táctica después de la Guerra de Corea, y la reconstrucción para Vietnam requirió un tiempo y un esfuerzo considerables. Ahora tenemos una capaci-

dad de soporte táctico ganada con esfuerzo que no debemos abandonar cuando nuestras miradas se dirigen al Pacífico.

Si los equipos de comunicaciones son adaptables, la cuestión se desplaza a la habilidad de nuestras tripulaciones de ser flexibles entre las dos misiones. ¿Han atrofiado nuestras habilidades estratégicas nuestra concentración en la contrainsurgencia durante los últimos 11 años? Sin duda, la Fuerza Aérea no ha abandonado completamente la misión estratégica, pero durante más de 20 años, la preponderancia de sus esfuerzos se ha basado en Oriente Próximo y Afganistán. Como en Corea y Vietnam, la necesidad de suministrar inteligencia a tiempo directamente al combatiente ha impulsado las tácticas, las técnicas y los procedimientos de la tripulación de hoy. Los aviadores jóvenes de hoy de ISR en vuelo han llevado a cabo siempre la misión táctica; para ellos, cambiar a la estratégica exigirá un considerable readiestramiento. Nuestros aviadores son muy inteligentes, pero el combate actual requiere un nivel de análisis muy fino. El suministro de una inteligencia oportuna ha reproducido una fuerza de lingüistas con pocas habilidades analíticas. La recopilación estratégica precipitará una vuelta a los días de análisis e informes metódicos más lentos—el reaprendizaje de esa habilidad también llevará tiempo.

La historia ha mostrado que los aviadores de ISR en vuelo son más que capaces de efectuar la transición de recopilación estratégica. A medida que las misiones vacilaban entre la recopilación estratégica de la Guerra Fría y las incursiones tácticas (Corea y Vietnam), nuestros antepasados de ISR en vuelo con operadores humanos tuvieron el lujo de deshacerse del conjunto de habilidades tácticas cuando volvieron a una recopilación estratégica. Las tripulaciones de ISR modernas no tendrán tanta suerte. Debido a la incertidumbre del entorno medioambiental, la Fuerza Aérea debe mantener sus capacidades tácticas. Nuestra fuerza incluye parte de los mejores talentos de esta nación; como sus predecesores, sin duda tienen la aptitud de efectuar la transición. Pero no podemos compensar un vacío de 11 años de la misión de recopilación estratégica de un día para otro. La lucha táctica de hoy exige una diseminación rápida de la inteligencia con poco enfoque analítico profundo. Las misiones estratégicas de mañana serán diferentes. Como en el caso de la Guerra Fría, los encargados de las decisiones a nivel nacional necesitan una inteligencia desarrollada de forma completa. En consecuencia, las fuerzas de ISR con operadores humanos deben cambiar su mentalidad para adaptarlas. Estos aviadores tendrán que aprender y volver a aprender habilidades lingüísticas, analíticas e informativas enfocadas estratégicamente. El paso del tipo de inteligencia rápido de un vistazo que es característico de las misiones actuales al que requiere paciencia y desarrollo de objetivos no será fácil. No obstante, no podemos efectuar un cambio absoluto a la estratégica. Según se mencionó arriba, debemos poder volver a la misión táctica como lo demandan las exigencias del entorno dinámico de hoy. Hacer esto requiere mucho de nuestros aviadores de ISR. Como siempre, tendrán éxito, pero es esencial que nuestros líderes les den el tiempo, el personal y los recursos que necesitan. □

Notas

1. Departamento de Defensa, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense (Sostenimiento de la prioridades de liderazgo global de EE.UU. para la defensa del siglo XXI)* (Washington, DC: Departamento de Defensa, enero de 2012), 2, <http://permanent.access.gpo.gov/gpo18079/DefenseStrategicGuidance.pdf>.

2. Marcus Weisgerber, “21st Century Rivet Joint” (Rivet Joint del siglo XXI), *Revista de la Fuerza Aérea* 94, no. 1 (enero de 2011): 52–54, <http://www.airforce-magazine.com/MagazineArchive/Documents/2011/January%202011/0111rivet.pdf>.

3. John H. Morrow Jr., *The Great War in the Air: Military Aviation from 1909 to 1921 (La Gran Guerra en el aire: la aviación militar de 1909 a 1921)* (Washington, DC: Smithsonian Institute Press, 1993), 60.

4. Lee Kennett, *The First Air War: 1914–1918 (La primera guerra aérea; 1914–1918)* (New York: Free Press, 1991), 30.

5. Eric Lawson y Jane Lawson, *The First Air Campaign: August 1914–November 1918 (La primera campaña aérea: agosto de 1914 a noviembre de 1918)* (Conshohocken, PA: Combined Books, 1996), 11.

6. *Ibid.*

7. *Ibid.*, 40.

8. Earle Rice Jr., *The First Battle of the Marne (La Primera Batalla del Marne)* (Filadelfia: Chelsea House, 2002), 93.

9. Benjamin D. Foulois, "The Tactical and Strategical Value of Dirigible Balloons and Dynamical Flying Machines" (El valor táctico y estratégico de los dirigibles y las máquinas de vuelo dinámico) (tesis, United States Army Signal Corps School, 1º de diciembre 1907), 3, 168.68-14, Agencia de Investigaciones Históricas de la Fuerza Aérea (AFHRA), Maxwell AFB, AL.

10. Kennett, *First Air War (La primera guerra aérea)*, 33.

11. Peter Mead, *The Eye in the Air: History of Air Observation and Reconnaissance for the Army, 1785-1945 (El ojo en el aire: historia de la observación y el reconocimiento aéreos para el ejército, 1785-1945)* (Londres: Her Majesty's Stationery Office, 1983), 66.

12. Kennett, *First Air War (La primera guerra aérea)*, 30.

13. I. B. Holley Jr., *Ideas and Weapons: Exploitation of the Aerial Weapon by the United States during World War I (Ideas y armas: explotación del arma aérea por Estados Unidos durante la PGM)* (New Haven, CT: Yale University Press, 1953), 149; y el Dr. Robert F. Futrell, *Command of Observation Aviation: A Study in Control of Tactical Airpower (Comando de aviación de observación: un estudio de control del poder aéreo táctico)*, Estudios Históricos de la Fuerza Aérea de EE.UU., no. 24 (Maxwell AFB, AL: Instituto de Estudios de Investigación, División Histórica de la Fuerza Aérea de EE.UU., Air University, 1956), 2, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA529959&Location=U2&doc=GetTRDoc.pdf>.

14. I. B. Holley Jr., *Evolution of the Liaison-Type Airplane, 1917-1944 (Evolución del avión tipo enlace, 1917-1944)*, Estudios Históricos de la Fuerza Aérea del Ejército, no. 44 (Washington, DC: Oficina Histórica de las Fuerzas Aéreas del Ejército, 1946), 8, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA529945&Location=U2&doc=GetTRDoc.pdf>.

15. Aileen Clayton, *The Enemy Is Listening (El enemigo está escuchando)* (New York: Ballantine Books, 1980), 212.

16. Alexander S. Cochran Jr., Robert C. Ehrhart y John F. Kreis, "The Tools of Air Intelligence: ULTRA, MAGIC, Photographic Assessment, and the Y-Service" (Las herramientas de la inteligencia aérea: ULTRA, MAGIC, evaluación fotográfica y el servicio Y), en *Piercing the Fog: Intelligence and Army Air Forces Operations in World War II (Perforación de la niebla: operaciones de las fuerzas aéreas de inteligencia y del Ejército en la Segunda Guerra Mundial)*, ed. John F. Kreis (Bolling AFB, Washington, DC: Programa de Historia de Museos de la Fuerza Aérea, 1996), 97, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA442835&Location=U2&doc=GetTRDoc.pdf>.

17. Cita en William E. Burrows, *By Any Means Necessary: America's Secret Air War in the Cold War (Por cualquier medio necesario: la guerra aérea secreta en la Guerra Fría)* (New York: Farrar, Straus y Giroux, 2001), 85-86.

18. Para obtener información adicional sobre lingüistas en vuelo, vea James C. McNaughton, *Nisei Linguists: Japanese Americans in the Military Intelligence Service during World War II (Lingüistas nisei: estadounidenses de origen japonés en el servicio de inteligencia militar durante la Segunda Guerra Mundial)* (Washington, DC: Departamento del Ejército, 2006), 371.

19. "The Contribution of Air Power to the Defeat of Germany" (La contribución del poder aéreo a la derrota de Alemania), apéndice M, Diversos aspectos del poder aéreo, 1, Jefe de Estado Mayor Asistente, A-2, Comandancia de las Fuerzas Aéreas de Estados Unidos en Europa, n.d., Carl Spaatz Papers, Box 274, Biblioteca del Congreso.

20. John T. Greenwood, "The Atomic Bomb—Early Air Force Thinking and the Strategic Air Force, August 1945–March 1946" (La bomba atómica—Primeros pensamientos de la Fuerza Aérea y la Fuerza Aérea estratégica, agosto de 1945 a marzo de 1946), *Aerospace Historian* 34, no. 3 (septiembre de 1987): 161.

21. Al principio de la Guerra Fría, los buscadores de objetivos estadounidenses y británicos se basaban en carpetas de objetivos capturados a la Luftwaffe y fotos de reconocimiento de áreas industriales rusas.

22. Robert J. Boyd, "Project Casey Jones, Post-Hostilities Aerial Mapping" (Proyecto Casey Jones, mapas aéreos posteriores a las hostilidades), informe del Mando de Aire Estratégico, 30 de septiembre de 1988, 1, K416.04-38, AFHRA.

23. *Ibid.*

24. Teniente Coronel George H. Peck, jefe, Relación de Medios y Civiles, Oficina de Asuntos Públicos, Mando de Aire Estratégico, Comandancia de USAFHRC y Comandancia SAC/HO, carta, "Asunto: Envío de manuscrito para el registro histórico", 20 de octubre de 1988, K-SQ-PHOTO-72-SU-PE, AFHRA.

25. Norman Polmar, *Spyplane: The U-2 History Declassified (El avión espía: historia del U-2 desclasificado)* (Osceola, WI: MBI Publishing, 2001), 6.

26. Alwyn T. Lloyd, *The Cold War Legacy: A Tribute to Strategic Air Command, 1946-1992 (Un tributo al comando de aire estratégico, 1946-1992)* (Missoula, MT: Pictorial Histories, 1999), 68.

27. *Ibid.*

28. Había excepciones, por supuesto; el SR-71 fue famoso por su sobrevuelo de territorio denegado.

29. Durante la Guerra Fría, los soviéticos derribaron al menos 13 aviones de reconocimiento de EE.UU. Para obtener información adicional, vea Michael L. Peterson, "Maybe You Had to Be There: The SIGINT on Thirteen Soviet Shootdowns of U.S. Reconnaissance Aircraft" (Tal vez usted tuvo que estar allí: la SIGINT en trece derribos soviéticos de la aviación de reconocimiento de EE.UU.) *Cryptologic Quarterly*, verano de 1993, 1, http://www.fas.org/irp/nsa/maybe_declass.pdf.

30. Hay excepciones: se debe informar sobre algunos tipos de inteligencia a los 10 minutos como máximo de una interceptación.

31. Historia, primer escuadrón de radio móvil, 1º de agosto de 1949–30 abril de 1950, 160.032-76, AFHRA.

32. Thomas L. Burns, *The Origins of the National Security Agency: 1940-1952 (Los orígenes de la Agencia de Seguridad Nacional, 1940-1952)*, Historia Criptológica de Estados Unidos, serie 5, vol. 1 (Fort Meade, MD: Centro para la Historia Criptológica, Agencia de Seguridad Nacional, 1990), 85, http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf.

33. Comandancia del USAFSS, *A Special Study: Securing Air Force Communications, 1948-1958 (Un estudio especial: cómo asegurar las comunicaciones de la fuerza aérea, 1948-1958)*, vol. 1, 1º de abril de 1966, 37.
34. Warren A. Trest, *Air Commando One: Heinie Aderholt and America's Secret Air Wars (Comando aéreo uno: Heinie Aderholt y las guerras aéreas secretas de EE.UU.)*; (Washington, DC: Smithsonian Institute Press, 2000), 34.
35. Michael E. Haas, *Apollo's Warriors: US Air Force Special Operations during the Cold War (Los guerreros de Apolo: operaciones especiales de la Fuerza Aérea de EE.UU. durante la Guerra Fría)* (Maxwell AFB, AL: Air University Press, 1997), 26, http://aupress.au.af.mil/digital/pdf/book/b_0037_haas_apollos_warriors.pdf.
36. Trest, *Air Commando One (Comando aéreo uno)*, 42-43.
37. Historia, Grupo de control táctico 6147, 1º de enero-30 de junio de 1953, K-GP-TACT-6147-HI, AFHRA.
38. Robert Frank Futrell, *The United States Air Force in Korea, 1950-1953 (La Fuerza Aérea de Estados Unidos en Corea, 1950-1953)* (Washington, DC: Office of Air Force History, 1983), 343.
39. J. Farmer y M. J. Strumwasser, *The Evolution of the Airborne Forward Air Controller: An Analysis of Mosquito Operations in Korea (La evolución del controlador aéreo avanzado en vuelo: un análisis de las operaciones Mosquito en Corea)* (Santa Monica, CA: RAND Corporation, 1967), 39, http://www.rand.org/pubs/research_memoranda/2005/RM5430.pdf.
40. El grupo de seguridad 6920, una organización del USAFSS, supervisó las operaciones del primer escuadrón móvil de radio en Corea.
41. Larry Tart y Robert Keefe, *The Price of Vigilance: Attacks on American Surveillance Flights (El precio de la vigilancia; ataques a los vuelos de vigilancia de EE.UU.)* (New York: Ballantine Books, 2001), 196.
42. *Ibid.*, 198.
43. *Ibid.*, 197.
44. General de División Doyle E. Larson, "Proyecto Teaball", notas sin publicar, n.d., 1 (obtenido mediante solicitud de la Ley de Libertad e Información).
45. General de División Doyle E. Larson, "Direct Intelligence Combat Support in Vietnam: Project Teaball" (Soporte de combate de inteligencia directa en Vietnam: Proyecto Teaball), *American Intelligence Journal* 15, no. 1 (Primavera/Verano de 1994): 57.
46. Robert J. Hanyok, *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975 (Espartanos en la oscuridad: la SIGINT de EE.UU. y la Guerra de Indochina)*, Historia Criptológica de Estados Unidos, Serie 6, Período NSA: 1952-presente, vol. 7 (Fort Meade, MD: Centro para la Historia Criptológica, Agencia de Seguridad Nacional, 2002), 273, <http://handle.dtic.mil/100.2/ADA483675>.
47. Larson, "Direct Intelligence Combat Support" (Soporte de combate de inteligencia directa), 57.
48. Hanyok, *Spartans in Darkness (Espartanos en la oscuridad)*, 274.
49. Larson, "Direct Intelligence Combat Support" (Soporte de combate de inteligencia directa), 58.
50. *Ibid.*
51. Cita en Marshall L. Michel III, *Clashes: Air Combat over North Vietnam, 1965-1972 (Confrontaciones: combate aéreo sobre Vietnam del Norte, 1965-1972)*, (Annapolis, MD: Naval Institute Press, 1997), 283.
52. Hanyok, *Spartans in Darkness (Espartanos en la oscuridad)*, 274.
53. Richard W. Stewart, *Operation Urgent Fury: The Invasion of Grenada, October 1983 (Operación Furia Urgente; la invasión de Granada, octubre de 1983)*, (Washington, DC: Centro de Historia Militar del Ejército de EE.UU., 2010), 10, http://www.history.army.mil/html/books/grenada/urgent_fury.pdf.



El Mayor Tyler Morton, USAF (BA, Universidad de Nebraska-Omaha; MS, Troy University; MMOAS, Air Command and Staff College; MPhil, School of Advanced Air and Space Studies) es un oficial de inteligencia profesional que trabaja actualmente como estratega de inteligencia, vigilancia y reconocimiento (ISR) en la Comandancia de la Fuerza Aérea. Al haber servido en la comunidad de ISR en vuelo durante gran parte de su carrera, como oficial y lingüista alistado, tiene más de 2.100 horas de vuelo en el RC-135 Rivet Joint. El Mayor Morton está cursando un doctorado en la Air University; su disertación es un análisis histórico de la evolución de las funciones de ISR en vuelo.

La Aviación y el Espacio Cibernético— Convergencia de Ámbitos, Convergencia de Amenazas

EMILIO IASIELLO

Introducción

La amenaza cibernética es uno de los peligros más comentados que enfrenta la comunidad internacional porque es global en alcance e impacta cualquier organización pública o privada que utiliza la *Internet*. Es un entorno que favorece al delincuente ya que hay pocas e ineficaces leyes que rigen la actividad que atraviesan las redes interconectadas, creando un ámbito funcional y sin fronteras. Como tal, los malhechores operan en un entorno oscuro donde sus actos se pueden esconder en grandes volúmenes de tráfico en la *Internet*. Los creadores de *malware* fabrican y venden sus creaciones sofisticadas, y no tan sofisticadas, en el mercado negro a actores de varios niveles de destreza para emplearlo en una amplia variedad de actividades hostiles que incluyen la perdurabilidad de la delincuencia cibernética; operaciones *hacktivistas* motivadas política o ideológicamente o el acceso oculto a redes y el robo de propiedad intelectual y documentos reservados que apoyan el espionaje industrial o de la nación estado. Recordando el viejo oeste de Estados Unidos de fines de los años 1800, no hay una presencia policial ni leyes penales comúnmente aceptadas que mantengan a los malhechores bajo control. Como resultado, los gobiernos extranjeros han reconocido la importancia de asegurar sus propias partes de esta red global, y algunos de ellos han redactado, o están redactando, estrategias nacionales de seguridad cibernética para tratar esta amenaza complicada y enigmática. Estados Unidos en particular ha tomado iniciativas agresivas para convertir la cibernética en un problema militar, esbozando en su *International Strategy for Cyberspace* (Estrategia internacional para el ciberespacio) de mayo de 2011 que “se reserva el derecho de emplear todos los medios necesarios—diplomático, informático, militar y económico—según sea prudente y consistente con las leyes internacionales pertinentes”.¹ Si bien es un primer paso positivo, el panorama comercial estadounidense permanece fragmentado y tribal en términos de seguridad cibernética de la organización, según se comprobó en los 15 Centros de Análisis e Intercambio de Información (ISAC; por sus siglas en inglés) establecidos federalmente y específicos a la industria² cuya misión es proporcionar información precisa y oportuna a los miembros interesados de la infraestructura crítica. El ISAC de Transporte (PT ISAC, por sus siglas en inglés) en particular tiene una labor ingrata de tratar de llevar a cabo esta función a lo largo de todos los sistemas de transporte público. A medida que las aeronaves se modernizan y adoptan la capacidad de operaciones interconectadas, la aviación confrontará actores hostiles, vulnerabilidades de equipo, *malware* programado, actividad maliciosa y retos de seguridad relacionados con este panorama de amenaza nuevo. En lugar de reaccionar a este entorno de amenaza dinámico y complejo, la aviación necesita tratar de manera preventiva las amenazas cibernéticas para adelantarse al problema o de lo contrario arriesgar ponerse al día en un entorno donde los malos están escondidos y las actividades hostiles ocurren en nanosegundos.

Incidentes cibernéticos en la aviación que deben mencionarse

La industria de la aviación—y en particular el proceso de viajes aéreos—ha tenido el lujo inesperado de no ser el objetivo de ataques visibles y considerables. Si bien ha habido incidentes bien difundidos de supuesto espionaje cibernético, los actores que buscan lograr el acceso no autorizado en la base industrial de la aviación, no ha habido informes similares perceptibles de actores hostiles atacando una *aeronave en movimiento*; o sea, de pista a pista. La aviación necesita considerar esto como una gran oportunidad para tratar las fallas de seguridad cibernética en el equipo, comunicaciones o cualquier punto de acceso que pueda ser aprovechado por actores técnicamente experimentados. En el 2011 hubo varios incidentes notables de actores hostiles dirigiendo sus operaciones cibernéticas malvadas contra los intereses de la aviación. Se sospecha que la mayoría de ellos fueron llevados a cabo por actores de espionaje ya que la mayoría se enfocaron en lograr acceso no autorizado a redes para fines de recopilación de información consistente con el comportamiento de actores de espionaje. No mostraron una intención destructiva típica de un *hacktivista* (por ejemplo, mediante ataques distribuidos de negación de servicio, degradación de un sitio *web*, etc.), ni tampoco implementaron campañas de *spam* de correo electrónico y correos electrónicos con virus *Trojan* para lograr acceso y obtener información personal identificable para fines de monetización como lo hacen típicamente los delincuentes cibernéticos.

- **Abril de 2011:** *L-3 Communications* fue el blanco de *hackers* utilizando *SecurIDs* comprometidos, un sistema de autenticación de dos factores. *L-3* no tenía claro si el ataque tuvo o no éxito, pero el evento fue significativo en que fue la primera vez que se utilizaban *SecurIDs* para intentar lograr acceso a una red.³
- **Mayo de 2011:** *Lockheed Martin* fue el blanco en una campaña de espionaje cibernético. Aparentemente, los agresores poseían las *seeds*—claves al azar codificadas por el fabricante—utilizadas por al menos algunos de los mandos (*job*) de *hardware* de *SecurID*, al igual que números de serie y el algoritmo subyacente utilizado para asegurar los dispositivos. Esta actividad fue detectada de manera oportuna y no hubo informes de que la información fuese robada o comprometida.⁴
- **Mayo de 2011:** *Northrop Grumman* fue el blanco en una campaña de espionaje cibernético similar a la de *Lockheed Martin*. Los agresores trataron de lograr acceso empleando *RSA Seeds* comprometidas. La actividad fue detectada antes de que se pudiesen robar la información.⁵
- **Octubre de 2011:** Un virus de computadora infectó las cabinas de los vehículos no tripulados estadounidenses, *Predatory Reaper*, anotando todas las pulsaciones de los pilotos a medida que volaban misiones por control remoto sobre Afganistán y otras zonas de guerra. La remoción del virus requirió múltiples esfuerzos indicando que el virus era resistente a la mitigación.⁶
- **Diciembre de 2011:** Irán alega haber explotado una vulnerabilidad conocida del GPS para engañar al vehículo no tripulado para que aterrizara en Irán.⁷

Tal como se ilustra en los ejemplos anteriores, no ha habido un ejemplo real de un actor hostil intentando impactar una aeronave durante el proceso del viaje aéreo. Sin embargo, si analizamos el progreso del entorno de la amenaza cibernética, podemos apreciar un paisaje dinámico donde los malhechores han aumentado continuamente sus capacidades y actividades en muy poco tiempo. El *malware* en sí ha cambiado dramáticamente. Desde el *Morris Worm* de 1988 cuyas consecuencias no intencionales causaron ataques de negación de servicio, hasta el descubrimiento del *Stuxnet* en el 2010, concebido para atacar *software* y equipo industrial específico, muestra cuán rápido las armas cibernéticas han logrado un nivel sofisticado de emplazamiento de armas.

Fecha	Fuente	Ataque	Blanco	Vector
6 de abril de 2011	 China	Comunicaciones L-3 Un correo electrónico con fecha del 6 de abril, enviado a 5000 empleados del contratista L-3 del DOD de E.UU., advierte sobre un intento de ataque efectuado con SecurID Seeds comprometidos. No está claro si el ataque tuvo éxito (fue revelado medio mes antes). Este es el primer ataque hecho con semillas RSA comprometidas.		SecurID comprometidas
21 de mayo de 2011	 China	Lockheed Martin Este es el primer ataque que se conoce (y el único reconocido oficialmente hasta el momento) perpetrado con semillas SecurID comprometidas que atacan a un contratista de la Defensa. El ataque fue detectado antes de que pudiesen robar información clasificada. Como precaución, se cerraron 100.000 cuentas.		SecurID comprometidas
26 de mayo de 2011	 China	Northrop Grumman Tercer contratista de la Defensa atacado utilizando semillas RSA comprometidas. El ataque fue detectado antes de que pudiesen robar información clasificada. El acceso remoto fue cerrado.		SecurID comprometidas
8 de octubre de 2011	? Se desconoce	Vehículos aéreos no tripulados estadounidenses Un virus de computadora infectó las cabinas de los vehículos no tripulados estadounidenses, Predator y Reaper, anotando todas las pulsaciones de los pilotos a medida que volaban misiones por control remoto sobre Afganistán y otras zonas de guerra. El virus fue detectado hace dos semanas en el Sistema de Control Terrestre (GCS) en la Base Aérea Creech, Nevada, y no ha interrumpido las misiones de vuelo de los vehículos aéreos no tripulados, mostrando una fortaleza inesperada de manera que múltiples intentos fueron necesarios para eliminar el virus de las computadoras en Creech.		Malware genérico a través de un USB stick
9 de diciembre de 2011	 Irán	Lockheed Martin RQ-170 Sentinel Un RQ-170 Sentinel hace un aterrizaje forzoso en Irán. Después de unos días, según informes del Christian Science Monitor, Irán pudo capturar el RQ-170 estadounidense explotando una vulnerabilidad conocida en el GPS, engañando a la aeronave a que aterrizara en Irán.		¿Piratería al GPS?

Figura 1. Lista de algunas actividades notables producidas por Hackmageddon.com⁸

Incidentes en aeropuertos que deben mencionarse

Los aeropuertos han sido víctimas de supuestas actividades ilícitas por parte de actores. En un aeropuerto hay muchos posibles puntos de entrada digitales que pueden ser el blanco para la interrupción. Las comunicaciones entre el control de tráfico aéreo y la aeronave, los servicios de abordaje y registro de pasajeros (que son accesibles en la *Internet*), los sistemas para procesar pasajeros, redes virtuales privadas en los aeropuertos (empleadas para asegurar las conexiones en la *Internet* entre la red privada de una organización y un empleado a distancia) y las redes inalámbricas son tan solo algunos de los sistemas dentro del entorno de un aeropuerto que pueden ser atacados y explotados para fines viles. Algunos incidentes recientes destacan la posible amenaza de actores hostiles tratando de lograr el acceso no autorizado a las redes de los aeropuertos.

- **Agosto de 2012:** Una empresa de seguridad digital en Boston descubrió un *malware* escondido en la red virtual privada (VPN, por sus siglas en inglés) en un aeropuerto internacional importante fuera de Estados Unidos. La amenaza pudo haber comprometido todo, desde la información personal de los empleados hasta la seguridad de los pasajeros, alegó la empresa. El ataque empleó el *malware Citadel Trojan* para leer las pantallas de los empleados quienes se conectaron por control remoto a la red del aeropuerto.⁹

- **Junio de 2012:** *Software* de juego infectado fue dirigido por un servidor de comando para atacar el Aeropuerto Internacional Incheon de Corea del Sur en un intento de interrumpir el tráfico de vuelo vía un ataque *DDoS*.¹⁰
- **Junio de 2011:** Vuelos fueron afectados en la Terminal 3 del Aeropuerto Internacional Indira Gandhi cuando el Sistema de Procesamiento de Pasajeros de Uso General (CUPPS, por sus siglas en inglés) falló y estuvo sin funcionar por casi doce horas. Las investigaciones iniciales revelaron que el uso de un “código malicioso” de un lugar remoto desconocido causó la falla del CUPPS.¹¹

En dos de esas ocasiones, hubo poco conocimiento de los individuos responsables por los ataques. En el incidente de Corea del Sur, un hombre fue arrestado quien se presume haber comprado el *software* para juegos de agentes de inteligencia de Corea del Norte. Ya sea a sabiendas o no, estos ejemplos muestran el panorama variado de actores que pudiesen ser responsables de los ataques cibernéticos perpetrados contra los aeropuertos.

Actores de amenaza cibernética — ¿Quiénes son los malos?

El anonimato de la *Internet* proporciona una larga lista de actores estatales y no estatales que operan bajo un manto de oscuridad. Los ataques específicos y no específicos que originan de esas fuentes han afectado a los sectores público y privado alrededor del mundo. Si bien hay pruebas limitadas que esos actores atacan la aviación mediante medios cibernéticos, el volumen está sujeto al cambio basado en la intención del actor al igual que sus capacidades y los recursos necesarios para llevar a cabo esos ataques. Con base en la evolución del *hacking*, todos los sectores industriales estadounidenses han sido víctimas de actores viles en un momento u otro. La agricultura¹², la base industrial de la Defensa¹³, la energía¹⁴, finanzas¹⁵, el gobierno¹⁶, cuidado de la salud¹⁷, militares¹⁸, y el agua¹⁹ han enfrentado actividades cibernéticas hostiles de uno o más de los siguientes grupos de actores de amenaza:

- **Hactivistas:** Los *hactivistas* son *hackers* motivados política o ideológicamente para llevar a cabo actividades hostiles y a veces destructivas en apoyo a una causa o creencia. Grupos como *Anonymous* participan en operaciones contra blancos para castigar una transgresión percibida o llamar la atención a una situación. El comportamiento típico del *hactivista* incluye ataques de negación de servicio distribuido (DDoS, por sus siglas en inglés) que inunda el servidor de un sitio web de tanto tráfico que lo torna inoperable; degradación de sitios web, que es una forma de grafiti electrónico para enviar mensajes; *doxing* que es un proceso donde se roba y se publica en la *Internet* la información personal (por ejemplo, la dirección, número de teléfono e información personal identificable, etc.). Los *hactivistas* han demostrado repetidamente su voluntad para llevar a cabo operaciones cibernéticas ofensivas contra empresas que ellos piensan merecen servir de escarmiento. Si una aerolínea cae en la mira de un grupo *hactivista*, se espera que una actividad cibernética hostil, como mínimo, atacaría las páginas web de la aerolínea.
- **Hackers:** Los *hackers* (piratas cibernéticos) penetran las redes por la emoción del reto, o para alardear en la comunidad de *hackers*, entre otros motivos. Se diferencian de los *hactivistas* en que sus motivos no están basados ni en la política ni en la ideología. Si bien logran acceso a una red o computadora utilizada para requerir un nivel de destreza que separaba a los *hackers* expertos de los novatos, ahora los *hackers* pueden descargar *script* y protocolos de ataque de la *Internet* para lanzarlos contra los blancos.²⁰ Es más, esas herramientas para atacar se han tornado cada vez más sofisticadas a la vez que se han tornado más fáciles de utilizar, negando la necesidad de un individuo de ser un experto para lanzar ataques. Los sitios

de *hacking* cuentan con herramientas gratis, instrucciones y una plétora de *hackers* expertos que sirven de mentores para aquellos con menos experiencia.

- **Actores no estatales:** Los actores de naciones estados típicamente emplean el espionaje cibernético para recopilar información confidencial e información sobre la propiedad intelectual de sus blancos. Sin embargo, dependiendo de la intención de los actores de la nación estado, lograr acceso no autorizado a redes objetivos se puede aprovechar para hacer un reconocimiento y trazar un mapa de la red para poder obtener información de inteligencia para un ataque más adelante. Esto se considera el equivalente cibernético de “preparación de inteligencia del campo de batalla”.
- **Grupos terroristas:** Si bien los grupos y las organizaciones terroristas prefieren ataques cibernéticos contra sus blancos, hay un caudal de información cada vez mayor sobre el uso del ámbito cibernético por los terroristas. Principalmente, los terroristas emplean el ciberespacio para el reclutamiento, difusión de propaganda, provocación, radicalización, financiamiento, entrenamiento, planificación e investigación.²¹ Sin embargo, ciertos líderes terroristas a veces han exhortado a los islamistas radicales a que usen la *Internet* para fines más operacionales. En el 2004, Imam Samudra, el individuo responsable de manipular los bombardeos en el club nocturno en Bali, publicó una autobiografía detallando el uso de cometer delitos cibernéticos contra los intereses de Estados Unidos para llevar al país a la bancarrota.²² Después de la muerte de Osama Bin Laden en el 2012, un vídeo de Al-Qaeda promovió una *jihād* electrónica contra Estados Unidos.²³
- **Infiltrados:** Un infiltrado a sabiendas o no puede proveerles a los actores hostiles acceso directo a redes y sistemas que ellos quieren atacar para interrumpir, destruir o manipular. Según un estudio, ellos son las fuentes principales de delitos en computadora.²⁴ Los infiltrados son cualquier individuo que tiene acceso directo o indirecto a una computadora o red específica.

Amenazas futuras de *malware* y la aviación

Las amenazas cibernéticas a las redes críticas de la infraestructura continúan evolucionando a medida que el panorama global se torna cada vez más interconectado. Esencialmente, mientras más compleja y avanzada se torna la red, más fallas técnicas y vulnerabilidades contiene, y más difícil se torna administrarla desde un punto de vista de seguridad. La industria de la aviación está desplazándose hacia un entorno más interconectado para mejorar todos los aspectos de los viajes aéreos, desde una aeronave en tierra hasta el despegue. La Autoridad Federal de la Aviación de Estados Unidos calcula que para el 2020 la mayoría de las aeronaves civiles del mundo habrán implementado el Sistema de Difusión de Vigilancia Dependiente Automática (ADS-B, por sus siglas en inglés), una tecnología de vigilancia avanzada, que reemplazará al radar como el principal medio para rastrear aeronaves. Durante todos los aspectos del viaje, la información fluirá a través de este entorno interconectado desde estaciones terrestres al control de tráfico aéreo a la aeronave en vuelo. Si bien no se podrá tener acceso a esta tecnología directamente vía la *Internet*, dos anécdotas de gran impacto revelan cómo actores duchos han diseñado herramientas cibernéticas para penetrar exitosamente e impactar sistemas que no son accesibles fácilmente vía la *Internet* sino de su propia red.

- **Stuxnet:** Descubierta en el 2010, *Stuxnet* es un gusano informático concebido para atacar los sistemas de control *Siemens*. Probablemente una memoria USB lo introdujo a la red cerrada.²⁵ El *malware* fue diseñado solamente para los sistemas de control de supervisión y adquisición de datos (SCADA, por sus siglas en inglés) que fueron configurados para controlar y moni-

torear procesos industriales específicos.²⁶ Esta fue la primera vez que un arma cibernética ataca un sistema de tipo específico e impacta con éxito sus operaciones. Este gusano dañó con éxito unas 1.000 centrifugas.

- **OPERACIÓN BUCKSHOT YANKEE:** En el 2008, el Departamento de Defensa de Estados Unidos sufrió un compromiso significativo de sus redes de computadoras militares clasificadas. Comenzó cuando una unidad *flash* fue insertada en una computadora portátil militar en una base en el Oriente Medio. El código malicioso de la unidad *flash*, colocado por una agencia de inteligencia extranjera, se cargó a sí mismo a una red administrada por el Comando Central de EE.UU. Ese código se esparció sin ser detectado en los sistemas clasificados y no clasificados, estableciendo el equivalente a un punto de partida digital del cual se pudiesen transferir datos a servidores bajo control extranjero.²⁷

Tan solo porque la industria de la aviación no ha sufrido un ataque cibernético sustancial como un *DDoS*, o un incidente como los descritos arriba, no significa que no puede suceder y no se debe dar por sentado que a causa de que las redes operacionales no están conectadas a la *Internet* que esos sistemas están protegidos del *malware*. Actos destructivos o perturbadores de *malware* (por ejemplo, *Stuxnet*, o el *malware Shamoon* del 2012 que barrió con 30.000 computadoras en la red saudí *Aramco*, borrando completamente los discos duros)²⁸ son tan solo una avenida disponible para los actores hostiles. A medida que la aviación adopta la tecnología ADS-B sumamente interconectada, varias fuentes de información serán enviadas al ADS-B incluyendo pero no limitado a las siguientes:

- **Tráfico:** Un piloto podrá tener acceso a información sobre el tráfico aéreo, incluyendo altitud, rumbo, velocidad y distancia a la aeronave.
- **Tiempo:** Las aeronaves equipadas con una tecnología UAT ADS-B podrán recibir informes de las condiciones del tiempo y del radar meteorológico mediante el servicio de difusión de información de vuelo (FIS-B, por sus siglas en inglés).
- **Terreno:** La tecnología ADS-B difunde una transparencia del terreno para que los pilotos la puedan ver en la cabina.
- **Información de vuelo:** No se debe confundir con FIS-B, servicio de difusión de información del tráfico (TIS-B, por sus siglas en inglés) transmite información de vuelo que se puede leer.²⁹

Toda mala interpretación o manipulación a sabiendas de información de vuelo crítica puede lograr resultados dañinos igual que cualquier otro ataque cibernético. Sin embargo, en este caso, la manipulación de datos puede ser un catalizador para ocasionar daños físicos a la aeronave e impactar directamente la seguridad de los pasajeros.

Conclusión

La industria de la aviación continúa progresando para crear un entorno en la *Internet* que interconecte exitosamente los componentes multifacéticos del panorama de la aviación. La revisión del Sistema Nacional Aeroespacial hará los viajes más convenientes y seguros, facilitando el intercambio de información a niveles sin precedente para informar mejor a los operadores y aumentar la eficacia a la vez que mantiene un nivel elevado de seguridad. Sin embargo, la tecnología involucrada en implementar un proceso de comunicaciones ininterrumpido provee una infinidad de oportunidades de las que los actores hostiles se pueden aprovechar. Aunque la aviación ha evadido con éxito la atención de actores cibernéticos hostiles, esto puede que cambie continuamente particularmente a medida que los entornos interconectados atraen el interés de actores que consideran la aviación como un blanco posible—actores de naciones estados

pueden atacar la aviación para el acceso para consideraciones futuras; los delincuentes cibernéticos pueden atacar la aviación para robar datos confidenciales o chantajear las operaciones de las aerolíneas para fines monetarios; y los *hacktivistas* pueden atacar la aviación para castigar las presuntas infracciones o para llamar la atención a sus causas políticas o ideológicas. El único factor constante entre estos actores es que son dinámicos, capaces de adaptarse rápidamente a sus entornos operativos. Si la aviación no ha sido atacada al punto que las otras lo han sido es porque estos actores aún no han reconocido cómo la aviación pudiese promover sus objetivos respectivos, y no porque no son capaces de hacerlo. La aviación está en una posición singular porque tiene la oportunidad de planificar para esas amenazas antes de que se tornen demasiado abrumantes o costosas de arreglar. Esperar para tratarlas porque aún no son un problema será equivalente a cerrar la puerta del establo cuando el caballo ya se ha escapado. □

Notas

1. The White House, *International Strategy for Cyberspace* (Estrategia Internacional para el Ciberespacio); mayo de 2011; consultado en: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
2. Página web del *National Council of ISACs*, consultada en: <http://www.isaccouncil.org/membersacs.html>.
3. William Jackson, "Another Major Defense Contractor Hacked, RSA Tokens Likely Involved" (Otro contrato importante de la defensa fue pirateado, *RSA Tokens* probablemente involucrados), *Government Computer News*, 1o de junio de 2011, consultado en: <http://gcen.com/Articles/2011/06/01/Defense-contractors-L3-Lockheed-hacked.aspx?p=1>.
4. Matthew J. Schwartz, "Lockheed Martin Suffers Major Cyberattack" (*Lockheed Martin* sufre otro ataque cibernético importante), *Information Week*, 31 de mayo de 2011, consultado en: <http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151>.
5. Jeremy Kaplan, "Northrop Grumman May Have Been Hit With a Cyberattack" (*Northrop Grumman* puede que haya sufrido ataque cibernético), *Fox News*, 1o de junio de 2011, consultado en: <http://www.foxnews.com/tech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/>.
6. Noah Shachtman, "Computer Virus Hits U.S. Drone Fleet" (Virus de computadora ataca flota de aviones no tripulados de EE.UU.), *Wired Magazine*, 7 de octubre de 2011, consultado en: <http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/>.
7. Scott Peterson, "Iran Hijacked US Drone, Says Iran Engineer" (Según ingeniero iraní, Irán secuestró aeronave no tripulada estadounidense), *Christian Science Monitor*, 15 de diciembre de 2011, consultado en: <http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video>.
8. *Hackmageddon.com*, consultado en: <http://hackmageddon.com/?s=aviation>.
9. Michael Dolgow, "Cyberwars Reach a New Frontier: The Airport" (Guerras cibernéticas alcanza frontera nueva: El aeropuerto), *Bloomberg Businessweek*, 15 de agosto de 2012, consultado en: <http://www.businessweek.com/printer/articles/67128-cyberwars-reach-a-new-frontier-the-airport>.
10. Jeff Goldman, "South Korean Man Arrested Over Airport Cyber Attacks" (Surcoreano arrestado por ataques cibernéticos al aeropuerto), *ESecurity Planet*, 5 de junio de 2012, consultado en: <http://www.esecurityplanet.com/print/network-security/south-korean-man-arrested-over-airport-cyber-attacks.html>.
11. Manan Kakkar, "CBI Believes Cyber Attack Led to IGI Airport's Technical Problems in June" (CBI cree que ataque cibernético fue causa de problemas técnicos en Aeropuerto IGI en junio), *ZdNet*, 25 de septiembre de 2011, consultado en: <http://www.zdnet.com/blog/india/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june/710>.
12. Eduard Kovacs, "US Department of Agriculture Sites Hacked in Protest Against Mohammed Movie" (Sitios web del Departamento de Agricultura de EE.UU. fueron pirateados en protesta contra película de Mahoma), *NewsSoftpedia*, 21 de septiembre de 2012, consultado en: [://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml](http://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml).
13. *Office of the National Counterintelligence Executive*, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace" (Espías extranjeros roban en el espacio cibernético secretos económicos de Estados Unidos), octubre de 2011, consultado en: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
14. Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber Espionage Campaign" (Se rumora que EE.UU. es el blanco de campaña masiva de espionaje cibernético), *Washington Post*, 10 de febrero de 2013, consultado en: <http://www.washingtonpost.com/archive/local/localnews/2013/02/10/>
15. Matthew J. Schwartz, "Bank Attackers Restart Operation Ababil DDoS Disruptions" (Los que atacaron banco comienzan nuevamente interrupciones DDoS Operación Ababil), *Information Week*, 6 de marzo de 2013, consultado en: <http://www.informationweek.com/security/attacks/bank-attackers-restart-operation-ababil/240150175>.

16. Bryan Krekel, “*Capabilities of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*” (Capacidades de la República Popular China para llevar a cabo guerra cibernética y explotación de redes de computadora), *US China Economic and Security Review Commission*, octubre de 2009, consultado en: http://www.dodea.edu/Offices/Safety/upload/14_china_spy.pdf.
17. RSA, “*Cybercrime and the Healthcare Industry*” (El delito cibernético y la industria del cuidado de la salud), 2010, consultado en: http://www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf.
18. Bob Orr, “*Pentagon Expands Cyber Defense Amid Daily Attacks*” (Pentágono amplía defensa cibernética en medio de ataques diarios), *CBS News*, 6 de febrero de 2013, consultado en: http://www.cbsnews.com/8301-18563_162-57568079/pentagon-expands-cyber-defense-amid-daily-attacks/.
19. Ellen Nakashima, “*Foreign Hackers Target U.S. Water Plant in Apparent Malicious Attack*” (*Hackers* extranjeros atacan sistema de agua potable en supuesto ataque malicioso), *Washington Post*, 18 de noviembre de 2011, consultado en: http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html.
20. *Government Accountability Office*, “*Cybersecurity: Threats Impacting the Nation*” (Seguridad cibernética: Amenazas que impactan a la nación), GAO-12-666T, 24 de abril de 2012, consultado en: <http://www.gao.gov/assets/600/590367.pdf>.
21. *United Nations Office on Drugs and Crime* “*The Use of the Internet for Terrorist Purposes*” (El uso de la *Internet* para fines terroristas), 2012, consultado en: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
22. Alan Sipress, “*An Indonesian’s Prison Memoir Takes Holy War into Cyberspace*” (Memorias de prisionero indonesio lleva Guerra Santa al espacio cibernético), *Washington Post*, 14 de diciembre de 2004, consultado en: <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>.
23. Jack Cloherty, “*Virtual Terrorism: Al-Qaeda Video Calls for Electronic Jihad*” (Terrorismo virtual: Video de al-Qaeda es un llamado a *jihad* electrónica), *ABC News*, 22 de mayo de 2012, disponible en: <http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875>.
24. *Government Accountability Office*, “*Cybersecurity: Threats Impacting the Nation*,” GAO-12-666T, 24 de abril de 2012, consultado en: <http://www.gao.gov/assets/600/590367.pdf>.
25. Robert McMillan, “*Siemens: Stuxnet Hits Industrial Systems*” (*Siemens Stuxnet* ataca sistemas industriales) *Computer World*, 14 de septiembre de 2010, consultado en: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142.
26. Nicholas Falliere, “*Stuxnet Introduces First Root Kit for Industrial Control Systems*” (*Stuxnet* introduce primer *root kit* para sistemas industriales de control), *Symantec*, 9 de agosto de 2010, consultado en: <http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>.
27. William J. Lynn, “*Defending a New Domain*” (Defendiendo un ámbito nuevo), *Foreign Affairs*, septiembre/octubre de 2010, consultado en: <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
28. *Reuters*, “*Saudi Aramco Says Hackers Too Aim at Its Production*” (*Aramco* saudí alega que *hackers* también quieren atacar su producción), *New York Times*, 9 de diciembre de 2012, consultado en: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.
29. *Federal Aviation Administration*, “*ADS-B Frequently Asked Questions*” (Preguntas comunes sobre ADS-B), consultado en: <http://www.faa.gov/nextgen/implementation/programs/adsb/faq/>.



El Sr. Emilio Iasiello es Jefe de Analista de Amenazas en iSIGHT Partner, una empresa global de inteligencia cibernética que brinda apoyo a entidades federales y comerciales para que administren riesgos cibernéticos, comprendan su entorno de la amenaza y les ayude a priorizar sus inversiones contra esas amenazas que impactan sus negocios o misión. Desde el 2002 ha trabajado en el análisis de amenazas cibernéticas tanto como contratista para el gobierno y en calidad de empleado civil con el Departamento de Estado y Departamento de Defensa respectivamente. Iasiello ha escrito varios artículos sobre el desarrollo de una nueva metodología analítica de amenazas cibernéticas y en la cadena de suministros IT.

Murió la Contrainsurgencia: ¿Qué más?

REMY MAUDUIT

En este lugar, el 26 de julio de 1972 el Ejército Real de Tailandia quemó todos sus libros de texto estadounidenses. De aquí comienza nuestra victoria sobre los comunistas.

—Inscripción sobre el incinerador
Cuartel General del Ejército Real de Tailandia

EL COMBATE ESTÁ llegando a su fin en Afganistán, y—como en Irak—han surgido serios cuestionamientos sobre el valor y la intención de la contrainsurgencia (COIN). Nos viene al recuerdo el lema “No más COINs” de la década de 1970, después de Vietnam. Las lecciones aprendidas nos deberían recordar hoy que debemos evitar tales guerras, pero es poco probable que lo hagamos en el futuro mejor de lo que hicimos en el pasado. Por tanto, quizás deberíamos pensar seriamente acerca de la causa fundamental de la forma más preponderante de conflicto: la insurgencia.

Teniendo en cuenta el impresionante número de libros sobre COIN, la abundancia de nuevas investigaciones sobre ex guerrilleros, doctrina militar, lecciones aprendidas, y la experiencia de quienes dirigieron las insurgencias (muy pocos) y COINs (demasiados), ¿entendemos mejor la guerra asimétrica?¹ El interés en este fenómeno se reduce a dos preguntas: (1) ¿Qué es una insurgencia? y (2) ¿Puede un ejército profesional triunfar sobre una insurgencia apoyándose en la población del país *donde se lleva a cabo la insurgencia*?

El desacuerdo abunda en casi todo aspecto de la guerra de insurgencia, incluyendo su definición. Evidentemente, los términos *guerra pequeña*, *guerra larga*, *guerra irregular*, *guerra asimétrica*, *terrorismo*, y otros, no delimitan el problema. La insurgencia los abarca a todos y más. Se desenvuelve en varias líneas de operación, cambia su énfasis, cambia la estrategia, o parece convertirse en una clase de conflicto diferente. La guerra insurgente se adapta, dependiendo del lugar de apoyo popular.

En primer lugar, una insurgencia tiene que ver con gente que comparte los mismos reclamos. Una fórmula subjetiva basada en la creencia de que el número de personas apoyan y se oponen a la insurgencia es igual, pero que la mayoría de la población permanece neutral, lista para ser reclutada, aún impregna las teorías y doctrinas de COIN. Tal fórmula fue producto de un enfoque académico, burocrático y una simplificación excesiva que hicieron algunos profesionales militares, basados en poca experiencia real y formados en un entorno muy distinto a una insurgencia. Tuvo enormes consecuencias que afectaron a las luchas COIN libradas por las potencias occidentales. Una formulación de este tipo es altamente arbitraria, y hasta cuestionable, por las siguientes razones:

1. La segmentación de la población en categorías es virtualmente imposible debido al secreto que un insurgente impone sobre sí mismo y la gente. Para adquirir la información que permita tal segmentación se requiere una inteligencia de COIN que supera la capacidad de las operaciones de inteligencia en un entorno de insurgencia.
2. La movilización del pueblo depende totalmente de las necesidades de la insurgencia en un momento y lugar específicos y de sus objetivos de corto y largo alcance.
3. El engaño es el punto fuerte de los insurgentes. En consecuencia, podrían estructurar la población para que se desempeñen como neutrales o colaboradores en los que el enemigo confía pero que en realidad apoyan la logística de insurgencia. Los insurgentes pueden

incluso animar a algunos de ellos a levantarse en armas contra la insurgencia, aunque en realidad los utilizan como fuente de inteligencia, municiones y lugares de descanso.

4. Podríamos comenzar con seguridad suponiendo que, con pocas excepciones, una insurgencia tiene el apoyo de toda la gente que comparte los mismos reclamos.

La causa fundamental de una insurgencia es un grupo de reclamos comunes muy enraizados entre los ciudadanos que pasan a ser los pretextos para el conflicto. La insurgencia se forma y crece si sus líderes establecen la conexión entre la lucha y las demandas de la población. Por tanto, los conflictos que se desarrollan dentro de la población civil se sustentan en ideas como justicia y libertad. Los insurgentes realizan actividades en un contexto explícitamente revolucionario que busca imponer un cambio radical en la situación actual mediante la subversión y la lucha armada.

La insurgencia saca fuerza de la ausencia de un “centro de gravedad”, un concepto que se enseña en las escuelas militares occidentales. La noción de un centro de guerra de Carl von Clausewitz se ha desplazado hacia una trilogía revolucionaria: (1) la voluntad de la gente como el centro de gravedad estratégico, (2) la voluntad del insurgente para continuar luchando como el centro de gravedad operativo, y (3) la multitud de células básicas de una organización clandestina como los muchos centros de gravedad tácticos. Estos centros de gravedad tienden a ser escalonados pero autónomos y secretos; por lo que la eliminación de cualquier centro de gravedad en cualquier nivel no puede contribuir a la caída de los otros, garantizando así la supervivencia de la insurgencia, independientemente del número de batallas o combatientes perdidos. Claramente, el deseo de ganar “los corazones y las mentes” de la población en una insurgencia se convierte en una ilusión peligrosa, un proceso de cambio cultural, y una miopía estratégica ingenua.

La meta de un ejército profesional es ganar guerras; la insurgencia parece haber arruinado esa misión. Las fuerzas armadas occidentales que participan en COIN han sido derrotadas o “se retiraron estratégicamente”. Proclamada por muchos expertos como la única victoria militar sobre una insurgencia, Malasia en realidad representa un caso exagerado; de acuerdo con el Dr. Andrew Mumford: “Una campaña de contrainsurgencia que tarda 12 años en erradicar a un grupo insurgente aislado no es un logro brillante y difícilmente merece los reconocimientos académicos que ha conseguido”.² Max Boot resume COIN observando que “la larga historia de conflictos de baja intensidad revela no solo lo omnipresente que han sido las guerras de guerrilla sino también la frecuencia con que se ha ignorado su importancia, creando así las condiciones para futuras humillaciones en manos de irregulares decididos”.³

Entonces, ¿qué más? Si seguimos considerando a la insurgencia como un asunto militar, debemos combatirla con medios militares especiales que estén libres de doctrina ambigua; comandos enormes y burocráticos; y expertos autoproclamados —es decir, con todo nuestro poderío militar, incluyendo el equipo y personal adecuados como inteligencia, fuerzas especiales y poderío aéreo. Quizás logremos mejores resultados que hasta el momento.

La “insurgencia preventiva” podría ser una opción incluso mejor. Los gobiernos no representativos crean agravios y reclamos, por lo tanto deberíamos alentar “vigorosamente” a nuestros amigos y aliados autocráticos para que cambien sus sistemas. Y si eso falla (como Egipto en el caso de Hosni Mubarak), deberíamos limitar el derramamiento de sangre e impedir que el segmento extremista de la población tome el control del país mediante el apoyo abierto a los insurgentes. Finalmente, debemos ayudar a construir estados-nación modernos que respondan a las necesidades de su pueblo. □

Notas

1. Rémy Madoui [también Mauduit], *J'ai été fellagha, officier français et déserteur: Du FLN à l'OAS* [Fui un insurgente, un oficial francés y un desertor: Del FLN a la OAS] (Paris: Éditions du Seuil, 4 April 2004).

2. Andrew Mumford, *Puncturing the Counterinsurgency Myth: Britain and Irregular Warfare in the Past, Present, and Future* (*Desinflando el mito de la contrainsurgencia: Gran Bretaña y la guerra irregular en el pasado, presente y futuro*), *Advancing Strategic Thought Series* (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, septiembre de 2011), 15, <http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1086>.

3. Max Boot, "The Evolution of Irregular War: Insurgents and Guerrillas from Akkadia to Afghanistan (La evolución de la guerra irregular: Insurgentes y guerrillas desde Acadia hasta Afganistán)", *Foreign Affairs*, Marzo/Abril de 2013, <http://www.cfr.org/afghanistan/evolution-irregular-war/p30087>.



El señor Remy Mauduit es editor de la edición África & Francophonie del Air & Space Power Journal y Presidente del Instituto Francés Guy P. Wyser de la US Marines University. Ha ofrecido charlas y cursos en Insurgencia y Contrainsurgencia en Escuelas Militares y Organismos de Gobierno en Estados Unidos y Francia. Mauduit pasó cinco años en posiciones de comando en insurgencia (Guerra de Argelia) y dos años en un Comando Francés de Contrainsurgencia. Mauduit recibió su nombramiento de una Escuela de Oficiales Francesa. Realizó estudios de posgrado (PhD/ABD) en Pennsylvania State University. Antes de unirse al ASPJ, Mauduit fue Vicepresidente de Operaciones y Mercadeo Internacional; Profesor asistente en DeSales University; Investigador y programador lingüístico en el Centro de Lingüística Aplicada/The Brookings Institution; Editor y presentador de TV para USIA; y Coordinador de idiomas del Cuerpo de Paz. Mauduit es un escritor con obras publicadas y autor de varios artículos.

Ataque Conjunto Inteligente en el Ciberespacio

MAYOR STEVEN J. SMART, USAF

A diario, Estados Unidos depende de nuestra infraestructura digital y proteger este recurso estratégico es una prioridad de seguridad nacional.

—Presidente Barack Obama, 2010

LA SEGURIDAD en el ciberespacio es una prioridad nacional evidente pero el papel que la milicia estadounidense desempeña en este ámbito nuevo no es tan claro. Con la activación en el 2010 del Comando Cibernético de Estados Unidos, el debate con respecto a la militarización del ciberespacio y la conducción de la “guerra” cibernética ha adquirido un papel protagónico entre los encargados de formular la política en el gobierno de EE.UU.¹ Complicando el asunto tenemos la práctica incierta del comportamiento del gobierno en el ciberespacio imponiendo pautas internas legales y políticas al igual que tratados internacionales con base en la guerra cinética.² A pesar de esta incertidumbre, la política del Departamento de Defensa (DOD, por sus siglas en inglés) exige que los componentes del DOD “cumplan con el derecho de guerra durante todos los conflictos armados, indistintamente de cómo se caractericen esos conflictos, y en todas las demás operaciones militares”.³ Aunque aún queda por ver cuáles roles y responsabilidades los encargados de formular la política en Washington, DC, harán para la milicia, el personal del DOD debe prepararse para llevar a cabo operaciones militares en el ámbito cibernético. Para hacerlo eficazmente, el Departamento debe aplicarles, con ligeras modificaciones, a las operaciones militares en el ciberespacio principios de ataque conjunto que han dado resultado anteriormente.⁴ En este artículo se analiza la eficacia de la *Joint Publication (JP) 3-60, Joint Targeting* (Publicación Conjunta (JP) 3-60, Selección conjunta de blancos), según aplica a las operaciones militares en el ciberespacio y propone recomendaciones para una doctrina conjunta de selección de blancos para el ciberespacio.⁵

Principios fundamentales de la selección conjunta de blancos

Antes de abordar la conveniencia de aplicar la JP 3-60 a la selección de blancos cibernética, debemos comprender sus principios fundamentales, la razón de aplicarlas y la relación entre la doctrina y la ley. “La doctrina conjunta presenta principios fundamentales que guían el empleo de las fuerzas militares estadounidenses”, y “(los comandantes) a todos los niveles deben garantizar que sus fuerzas operan según el ‘derecho de guerra’, la cual es obligatoria para Estados Unidos.”⁶ La doctrina conjunta incorpora lo que Estados Unidos ha acordado acatar en el derecho internacional al igual que las mejores prácticas operacionales. El “derecho de guerra” consta del derecho internacional convencional (tratados y acuerdos entre naciones estados) y el derecho internacional consuetudinario (basado en la práctica estatal).⁷ Este último surge de la práctica estatal, principalmente la conducta gubernamental oficial reflejada en una variedad de actos, inclusive la doctrina publicada. Por lo tanto, la doctrina conjunta no solo reafirma los compromisos legales obligatorios sino también fomenta el desarrollo del derecho internacional consuetudinario.

Para simplificar, los cánones principales que establecen la base para el derecho de guerra moderno están divididos entre reglas para la *conducción* de la guerra y el *trato* de las partes en el conflicto y sus testigos: las convenciones de la Haya y de Ginebra, respectivamente.⁸ Además, en

la Carta de las Naciones Unidas se esbozan las obligaciones de los estados miembros de la organización con respecto al “uso de la fuerza” contra otros estados.⁹ El derecho interno (los estatutos federales y las decisiones judiciales), las directrices del gobierno de EE.UU., la doctrina conjunta y de los servicios, al igual que las reglas de enfrentamiento (ROE, por sus siglas in inglés) especifican cómo las fuerzas militares estadounidenses cumplirán con esas obligaciones internacionales. Debemos comprender que ni la doctrina militar ni las ROE, ya sean permanentes o específicas a una misión, ni reemplazan ni sustituyen las leyes de guerra. Más bien, representan la puesta en vigor por parte de Estados Unidos de principios internacionales acordados a una situación específica.

Podemos sintetizar este conjunto de normas, regulaciones y doctrina en cinco principios sencillos que aplican a cualquier situación específica. Primero, el uso de la fuerza presupone la existencia de la *necesidad militar* (una razón militar válida para emplear la fuerza necesaria para llevar a cabo la misión).¹⁰ Segundo, el empleo de la fuerza propuesto no le debe ocasionar *sufrimiento innecesario* ni a la población civil ni a la fuerza enemiga objetivo.¹¹ Los comandantes deben implementar este principio—la base para convenciones futuras que prohíben el uso de ciertos tipos de armas y municiones (por ejemplo, armas químicas)—no solo a posibles “daños colaterales” (pérdida fortuita de vida civil o daño a la propiedad civil) sino también al objetivo propuesto del ataque. Tercero, el empleo de la fuerza debe discernir o distinguir entre combatientes y no combatientes al igual que evitar ataques intencionales contra las poblaciones civiles que no participan directamente en las hostilidades.¹² En pocas palabras, el operador debe usar un arma capaz de ser apuntada y debe distinguir entre civiles y adversarios—el principio subyacente que guía el análisis de la selección conjunta de blancos, la cual se explora más a fondo a continuación. Cuarto, la operación militar propuesta tiene que ser *proporcional*—es decir, debe evitar daños colaterales excesivos en virtud de la ventaja militar prevista.¹³ Por último las partes en el conflicto armado deben mantener el código de caballería o una “cierta cantidad de equidad... y un grado de respeto y confianza mutua”.¹⁴ Aplicar esos principios guía el empleo de la fuerza en general y las decisiones del ataque individual en particular.

En los círculos militares, el término *selección de blancos* a menudo describe una acción de una fuerza militar atacando, o preparándose para atacar, un adversario. Oficialmente, la doctrina conjunta define la selección de blancos como “el proceso de seleccionar y priorizar blancos y equiparar la respuesta correcta a ellos, tomando en cuenta los requerimientos y capacidades operacionales”.¹⁵ Esta definición, específicamente el proceso de seleccionar el blanco y equiparar la respuesta correcta al mismo, implican más directamente las obligaciones bajo el derecho de guerra. La selección de blancos es la premisa principal sobre la cual radica el principio de discriminación. Los *objetos* militares son blancos legítimos, pero las fuerzas no deben atacar a civiles intencionalmente y los deben salvar de efectos colaterales tanto como sea posible.¹⁶ Por lo tanto, el derecho de guerra responsabiliza tanto al comandante militar como al operador por identificar, caracterizar funcionalmente y atribuirle a un no combatiente, tan correctamente como sea práctico, la intención de una operación militar propuesta.

En la doctrina militar se establecen principios para guiar a las fuerzas en la conducción de sus obligaciones de discriminación. En la JP 3-60 se encuentran los principios globales de selección de blancos para llevar a cabo las operaciones combinadas o conjuntas. La doctrina del servicio militar, tales como el *Air Force Doctrine Document (AFDD) 2-1.9, Targeting* (Documento de Doctrina de la Fuerza Aérea (AFDD) 2-1.9, Selección de blancos), complementa la doctrina conjunta con principios diseñados específicamente para la responsabilidad principal del servicio individual.¹⁷ Esos principios emanan de las mejores prácticas, recurriendo a la experiencia colectiva de la milicia estadounidense y sus aliados durante campañas y operaciones militares anteriores. En vista de que ningún servicio militar tiene la responsabilidad primaria del ámbito ciberespacial y en vista de que hay pocas mejores prácticas colectivas, de haberlas, para las operaciones militares en el ciberespacio, la doctrina actual para otros ámbitos bélicos determina la planificación de la

operación ciberespacial e informa las decisiones de selección de blancos ciberespaciales.¹⁸ Por lo tanto, la JP 3-60 es *por omisión* la publicación fundamental actual sobre la selección conjunta de blancos en el ciberespacio.

Aplicación al ciberespacio

Aplicar la doctrina militar existente (específicamente, selección de blancos y principios del derecho de guerra) a las operaciones en el ciberespacio es fácil en teoría pero puede resultar extremadamente difícil en práctica. La ciberguerra difiere fundamentalmente del conflicto armado tradicional. A diferencia de la conducción de la guerra en el pasado, los opositores (inclusive actores estatales, criminales, terroristas y *hackers* [piratas informáticos]) pueden librar una ciberguerra desde lugares apartados en el globo rápida, económica, anónima y devastadoramente. La doctrina militar actual analiza las experiencias y teorías de la guerra *cinética* entre las naciones estados en espacios de batalla que existen casi exclusivamente en una zona físicamente reconocible y comprensible (aire, tierra, mar y espacio). Por el contrario, la guerra cibernética ocurre en “un ámbito ubicado simultáneamente en capas lógicas y físicas que cruzan actividades en, a través y que tienen que ver con el espectro electromagnético que cruza ininterrumpidamente otros ámbitos al igual que fronteras geográficas y políticamente reconocidas”.¹⁹

El punto hasta el cual la ciberguerra difiere de la guerra cinética y representa un cambio de paradigma en los asuntos militares modernos es un tema polémico más apropiado para los historiadores académicos. Sin embargo, hay diferencias entre los actores y los métodos del conflicto armado en el mundo físico y sus homólogos relacionados con los conflictos en el ciberespacio. Esas variaciones ilustran los retos complejos de aplicar la ley, política y doctrina militar vigentes a golpes de teclado y clics de ratón.

Primero, la participación en la ciberguerra no está limitada a los agentes de la nación estado. A diferencia del ataque militar convencional, llevar a cabo un ataque en el ciberespacio no requiere el patrocinio del gobierno.²⁰ Segundo, el agresor no necesita sistemas de armamento tradicionales costosos, solamente una computadora, una conexión a la *Internet* y experiencia cibernética básica.²¹ Tercero, a diferencia de atribuir un ataque en el mundo cinético, identificar la fuente de un ataque cibernético es sumamente difícil. Por ejemplo, encontrar a la nación agresora responsable de un ataque con misil es relativamente fácil porque “huellas” claves tales como el tamaño, velocidad, alcance y tipo de ojiva apuntan hacia una lista relativamente pequeña de países que cuentan con la tecnología, voluntad y experiencia para llevar a cabo ese tipo de ataque. Sin embargo, un ataque cibernético puede originar desde cualquier parte y por cualquiera, inclusive por “piratas informáticos” auspiciados por un estado, actores no estatales o “trabajadores por cuenta propia preparando un laptop golpe motivado políticamente”.²²

Las diferencias principales entre la ciberguerra y su prima, la guerra cinética, plantean preguntas pertinentes. Primero, ¿es realista esperar que inclusive operadores cibernéticos apoyados por el estado cumplan con los principios legales y la doctrina militar con base en nociones tradicionales de la guerra cinética en este nuevo ámbito? Segundo, ¿necesitamos una publicación conjunta nueva específicamente dedicada al ataque ciberespacial para justificar esas diferencias?

A pesar de las discrepancias en los ámbitos operacionales, los guerreros cibernéticos son básicamente lo mismo que sus homólogos en tierra, en el mar y en el aire. Ambos dependen de su conocimiento del ámbito, el entorno operacional y de las capacidades del sistema de armamento. La complejidad de librar una guerra resiste cualquier intento de reducirla a una lista de verificación estructurada para los comandantes. Los líderes astutos podrán discernir y aplicar las verdades duraderas de la guerra, inclusive el marco para su uso legal, dentro del contexto de un entorno operacional o estratégico en particular. Con unas pocas modificaciones, los operadores cibernéticos pueden aplicar principios legales y doctrina militar basada en la guerra cinética tradicional a las operaciones cibernéticas y aún producir los efectos previstos. De manera similar,

con solamente ligeros ajustes para las sutilezas cibernéticas, la JP 3-60 continúa sirviendo como la publicación fundamental de la milicia estadounidense para la localización cinética y no cinética de blancos.

La doctrina militar en el ciberespacio

En el pasado reciente, solamente una publicación conjunta se ocupaba exclusivamente de la conducción de las operaciones militares en el ámbito cibernético.²³ En la JP 3-13, *Information Operations* (Operaciones de Información), se identificaron las operaciones de información (IO, por sus siglas en inglés) como “el empleo integrado de la guerra electrónica (EW), operaciones en la red de computadoras (CNO), operaciones psicológicas (PSYOP), engaño militar (MILDEC) y operaciones de seguridad (OPSEC) en combinación con capacidades de apoyo y relacionadas especificadas para influenciar, interrumpir, corromper o usurpar la toma de decisiones humana y automatizada adversas a la vez que protegemos las nuestras”.²⁴ Doctrinalmente, las CNO, inclusive los ataques a la red de computadoras (CNA) y la defensa de la red de computadoras (CND), representaban tan solo un subconjunto de una categoría mayor de actividades que podría decirse no son similares. En la doctrina se reafirma la centralidad de esas capacidades a la IO en su totalidad, destacando que ayudarían al comandante de la fuerza a influenciar a un adversario. Pero agruparlas sugirió que la IO en sí es una especialidad bélica capaz de integrarse rápidamente a una fuerza de tarea conjunta. Lamentablemente, esta no es la manera como los servicios capacitan a su personal. Más bien, actualmente capacitan a un individuo en una o más aptitudes, tales como EW o PSYOP. Dentro de la CNO, rara vez una persona cuenta con pericia en CNA y CND. Por lo tanto, una célula IO a nivel de fuerza de tarea conjunta puede que conste de “cilindros de excelencia” (por ejemplo, individuos muy versados en su campo de entrenamiento limitado pero que poseen pocos conocimientos de las demás aptitudes). Esto es particularmente cierto con respecto al concepto de selección de blancos: la JP 3-13 no ofrece consejos sobre el tema.

Dado por hecho la naturaleza “básica” de esas capacidades, ¿por qué la JP 3-13 no incluye instrucción sobre la selección de blancos? Hay tres razones que acuden a la mente. Primero, la selección de blancos es tan esencial para la contienda que prácticamente todo miembro de la milicia tiene un entendimiento general del concepto. Sin embargo, la selección de blancos que logra exitosamente los objetivos tanto militares como políticos es un proceso sumamente complejo que relativamente pocos individuos han dominado. Sencillamente, la mayoría de los profesionales militares saben qué significa la selección de blancos, pero pocos saben cómo hacerlo. Segundo, en la JP 3-13 no se tratan los detalles de las aptitudes básicas. Más bien, refiere al planificador de IO a consultar otras publicaciones para recibir una guía, sugiriendo que esas aptitudes no están tan relacionadas como se afirma en la JP 3-13. En cambio, en las mentes de los planificadores militares convencionales, son tan solo son varias actividades militares singulares y poco convencionales difíciles de integrar en un plan de operaciones. Por último, muchos planificadores opinan que “la selección de blancos es selección de blancos”, indistintamente de la plataforma o ámbito.

La mayoría de los planificadores operacionales cibernéticos declararían que comprenden el concepto general de la selección de blancos según se considera en la definición oficial de la doctrina y según se esboza en la JP 3-60. No obstante, su aplicación del concepto y la definición a su capacidad IO básica podría significar algo muy diferente. Por ejemplo, una actividad PSYOP propuesta podría “seleccionar” una audiencia extranjera cuyo comportamiento y acciones los seleccionadores de objetivos desearían influenciar, pero una operación EW podría seleccionar señales de una torre de radio. En la JP 3-13 se sugiere que los cinco tipos de funciones IO mencionados anteriormente están relacionados entre sí pero no ofrecen pautas sobre cómo atacar al adversario empleando esas funciones específicamente.²⁵ El planificador u operador de la IO entonces debe acudir a otra publicación específica en el tema para obtener una guía.²⁶ El hecho de

que la JP 3-13 representa la única orientación conjunta sobre las operaciones en la red complica la cuestión para el planificador de CNO.²⁷ Por lo tanto, los planificadores de las CNO al nivel conjunto a menudo tienen que referirse a la doctrina del servicio para ese tipo de orientación.

Recientemente la Fuerza Aérea hizo público el AFDD 3-12, *Cyberspace Operations* (Operaciones Ciberespaciales), que distingue entre las operaciones cibernéticas y las de información.²⁸ Este documento representa el mejor intento del servicio para comprender, organizar, capacitar y orientar a los hombres del aire en las operaciones ciberespaciales. Lo suficientemente básico para el novato en cibernética, pero suficientemente exhaustivo para el experto, el AFDD 3-12 les ofrece a los hombres del aire orientación técnicamente sensata y operacionalmente relevante a falta de una orientación al nivel conjunto—una hazaña particularmente sorprendente. Más impresionante aún, el documento relaciona los principios de las operaciones conjuntas con las operaciones ciberespaciales, ofreciendo información a lo largo de la gamas de las operaciones militares y esbozando los principios fundamentales para el ciber guerrero de la Fuerza Aérea.²⁹ Podría decirse que el AFDD 3-12 es el documento más exhaustivo sobre las operaciones cibernéticas en el DOD: de hecho, la fuerza conjunta se favorecería con una publicación conjunta que tuviese su alcance y profundidad. Hay que reconocer que aunque en el AFDD 3-12 se discuten muchos temas útiles para la selección cibernética de objetivos, tales como las relaciones técnicas en la infraestructura ciberespacial, seguridad en la información, ciclos de decisión comprimidos y el reto del anonimato y la atribución, no se trata específicamente la selección cibernética de blancos.³⁰ De hecho, el documento refiere a los lectores a la JP 3-60, sugiriendo que los principios, orientaciones y teoría de la publicación conjunta aplican correctamente a las operaciones ciberespaciales de la Fuerza Aérea.

Por un lado, el tema de la selección de blancos rara vez aparece en la doctrina actual, conjunta o del DOD sobre el ciberespacio, quizás porque la milicia recientemente ha comenzado a organizar oficialmente sus ciber fuerzas o porque los servicios no cuentan con una experiencia extensa y colectiva a la cual recurrir sobre la selección cibernética de objetivos.³¹ Por otra parte, los líderes en el DOD puede que sencillamente opinen que los principios de selección de blancos de la JP 3-60 son tan sensatos que pueden traducirse fácilmente a las operaciones militares en el ámbito cibernético. Indistintamente de las razones, la JP 3-60 continúa siendo la publicación conjunta fundamental sobre la selección de blancos en el ciberespacio a pesar del hecho de que no hace ninguna referencia al ámbito en sí.

Repaso de la Publicación Conjunta JP 3-60

Organizada en tres secciones principales—fundamentos de la selección de blancos, el proceso conjunto de la selección de blancos y deberes y responsabilidades—la JP 3-60 pasa a explicar con lógica desde la definición del término *blanco*; a través de la selección de blancos, ataque al blanco y evaluación de daños, hasta responsabilidades de mando y supervisión. Un principiante en selección de objetivos captaría rápidamente los conceptos básicos de este documento conciso y bien redactado. Por ejemplo, una gráfica sencilla (figura II-I, Ciclo de selección conjunta de objetivos) transmite la esencia de la selección de blancos en combate.³² Comprender el ciclo es comprender la selección de blancos.

EL ciclo de la selección conjunta de blancos esboza rápidamente el quién, qué, dónde, cuándo, por qué y cómo del ataque del adversario.³³ Luego de que el comandante de la fuerza conjunta anuncie un *estado final* y un *objetivo*, los planificadores *elaboran* y *colocan en orden de prioridad* los blancos con tal fin. La selección de blancos impulsa la *correlación arma/capacidad* que garantiza el ataque exitoso a la vez que minimiza los daños colaterales. El arma en particular seleccionada define la *asignación de la fuerza*, que informa la *planificación de la misión* e impulsa la *ejecución*, después de lo cual una *evaluación* le informa al comandante si la misión ha cumplido los objetivos o si es necesario localizar más blancos, según se determine a través de la evaluación

de medidas de eficacia predeterminadas y medidas de rendimiento. Saltar pasos en el ciclo pone en peligro la eficacia de la misión; agregar pasos fuera del ciclo es superfluo. Desde un punto de vista legal, acatar el proceso del ciclo de selección conjunta de blancos y otros principios fundamentales en la publicación, junto con juicio de mando firme, prácticamente garantiza el cumplimiento con el derecho de guerra.

Por lo tanto, el JP 3-60 parece ser la “guía” tipo para seleccionar blancos en cualquier ámbito. Lamentablemente, un análisis que de por sentado que el ámbito cibernético comparte esencialmente las mismas características con el aire, tierra, mar y espacio no explica su singularidad.

Al igual que los demás ámbitos, el ciberespacio ocupa un área, está sujeto a la explotación por parte de gobiernos y empresarios y sirve como un medio para el intercambio de comercio entre las corporaciones, naciones e individuos. Sin embargo, este medio singular “tiene que ser apreciado por sus propios méritos; es un concepto hecho por el hombre”.³⁴ Las computadoras permiten acciones en casi tiempo real y puede que para el usuario provean una casi anonimidad. El hecho de que criminales, terroristas y actores estatales utilicen la misma infraestructura cibernética empleada por empresas comerciales e individuos para llevar a cabo sus operaciones le agrega un “contexto social” a las operaciones militares en este ámbito.³⁵ En los ámbitos del aire, espacio y mar relativamente pocos adversarios son lo suficientemente competentes como para amenazar o retar eficazmente a Estados Unidos y su milicia. Por el contrario, el ámbito cibernético está repleto de actores capaces de presionar, confrontar o intimidar a Estados Unidos, sus aliados y entre sí. Este espacio de batalla congestionado complica poder utilizar la JP 3-60 como una guía para la selección de blancos cibernética en cinco áreas clave: (1) identificación positiva de blancos, (2) ubicación de blancos, (3) atribución del ataque, (4) aparear la capacidad/blanco y (5) evaluación de posibles daños colaterales.

Primero, la complejidad de la infraestructura ciberespacial global de doble uso complica la identificación positiva de un posible blanco cibernético. Las dos secciones en la JP 3-60 que tratan la identificación de blancos—capítulo 2, “*The Joint Targeting Process*” (El proceso de selección conjunta de objetivos) y el Apéndice E, “*Legal Considerations in Targeting*” (Factores legales en la selección de blancos)—aclaran que un blanco militar válido y legal exige un grado de identificación y caracterización específica llevado a cabo durante un ciclo de selección de blancos o bien normal o dentro de un periodo de tiempo específico. Ninguna sección trata ni la naturaleza fugaz, ni la singularidad de los blancos cibernéticos ni destaca que éstos existen casi exclusivamente en un medio de uso doble.

A modo de ilustración, supongamos que los planificadores designan tres blancos a una junta conjunta de coordinación de blancos, un grupo que “facilita y coordina las actividades de selección de blancos de la fuerza conjunta. . . para garantizar que se cumplen con las prioridades del comandante de la fuerza conjunta”.³⁶ El primer blanco designado es un tanque, el segundo un sitio en *Internet* y el tercero un “personaje” en línea. Inicialmente, la junta podría validar el tanque como un blanco militar pero mantener que ni el sitio en *Internet* ni el personaje califican como blancos militares válidos según se contempla en la JP 3-60 o las leyes de guerra porque no son un objeto físico sino una fórmula compuesta de unos y ceros—una evaluación incorrecta. De hecho, la JP 3-60 no limita un blanco al mundo físico, en cambio lo define como “una entidad u objeto considerado para posible ataque o acción” (énfasis añadido).³⁷ Esta definición amplia abarca el sitio *Internet* y el personaje.

La legitimidad de atacar el tanque de un adversario está clara por la finalidad exclusiva de esa arma de destruir y neutralizar dentro de los confines del conflicto armado, pero un análisis del derecho de guerra del sitio en *Internet* y el personaje debe ir un paso más allá. Tanto el sitio en *Internet* como el personaje tendrían que pasar la prueba del “uso” en lugar de “propósito”—o sea, al momento del ataque propuesto, ¿está el adversario usándolos para promover sus capacidades de combate o de sostener la guerra? De ser así, entonces puede que sean los objetos legales de un ataque militar. El momento exacto de cuándo estos objetos de doble uso, entidades o com-

portamientos en y a través del ciberespacio en realidad contribuyen a la causa del adversario dificulta el enfrentamiento. A diferencia de la validación de blancos durante la guerra cinética, el proceso con los blancos cibernéticos exige tanto una actualización consistente de la inteligencia de validación y una identificación positiva en casi tiempo real.

Segundo, la ubicación de un blanco cibernético presenta retos singulares. En la JP 3-60 y en las leyes de guerra se trata la ubicación de blancos en el contexto de la invasión física de una nación soberana. Ni en la doctrina ni en la ley se contempla que un blanco exista en varios lugares diferentes alrededor del mundo a la misma vez o que cause efectos en teatros múltiples de conflicto, como puede suceder en el ciberespacio. Por ejemplo, un adversario puede llevar a cabo mando y control a través de sitios de *Internet* alojados simultáneamente en servidores en diferentes países y puede frustrar el ataque moviendo frecuentemente esos sitios de *Internet*. Problemáticamente, las ROE particulares que aplican al planificador militar puede que excluyan acciones en ciertos lugares fuera de la zona de operaciones conjuntas aunque el adversario utilice una red global siempre cambiante para lograr que los efectos ocurran. Este dilema conduce a un debate significativo e importante. ¿Cuál es el blanco? ¿Acaso es el adversario ubicado físicamente en la zona de operaciones conjuntas, o es su red de mando y control distribuida globalmente? Si la ubicación excluye el enfrentamiento, entonces el planificador militar naturalmente reevalúa el blanco exacto. ¿Acaso son las fuerzas en campaña o sus redes?

Tercero, la atribución de las capacidades cibernéticas, equipo y uso para una entidad en particular declarada hostil es difícil en el ciberespacio. Aunque la atribución puede caer bajo la identificación positiva, en este artículo se trata como un problema aparte para aclarar las diferencias entre la selección ofensiva y defensiva de blancos cibernéticos.³⁸ La anonimidad que el ciberespacio ofrece le permite al enemigo enmascarar sus acciones y atribuir las falsamente a un no combatiente o a cualquier otra entidad. Un adversario podría secuestrar las computadoras civiles inocentes, grupos o gobiernos y utilizarlas como una “red *botnet*” para lanzar un ciberataque. Una vez que la víctima del ataque lleva a cabo una investigación forense rudimentaria, la atribución del ataque señalaría a los no combatientes inocentes en lugar de al verdadero autor. Estrictamente hablando (dependiendo de la cantidad del daño), la ley de guerra consideraría un ataque de ese tipo como el crimen de guerra de perfidia. Hablando prácticamente, si el ataque fuese continuo (por ejemplo, una negación de servicio distribuida), ¿debe la víctima obtener la identificación positiva de cada blanco, atribuyéndolo en esencia a una entidad hostil declarada, antes de lanzar las medidas de defensiva a las computadoras que “atacan”? Afortunadamente, como se menciona arriba, la ley de guerra reconoce el derecho intrínseco de auto defensa (enfocándose en la ubicación de la amenaza) y no requiere una identificación positiva del agresor. Pero en el ciberespacio, inclusive una respuesta simple y llanamente defensiva a una computadora que ataca podría tener severas consecuencias en cascada y no intencionadas para la ciber infraestructura global—sin mencionar la pesadilla política de contraatacar la parte equivocada.

Cuarto, el apareamiento de la capacidad y el blanco en el ciberespacio involucra temas singulares. La acción ofensiva puede que requiera aptitudes de precisión para evitar daños colaterales significativos. Una postura defensiva (o respuesta en caso de crisis) puede que exija el uso de capacidades poderosas de contraataque y disuasión contra una amplia gama de agresores—creando más un *firewall* amplio en lugar de un ataque preciso.

Quinto, el arduo proceso de evaluar los posibles daños colaterales en el ciberespacio exige inteligencia significativa y la interconectividad de redes y redundancias en los sistemas que requieren una planificación meticulosa. Al momento no contamos con una metodología oficial para calcular daños colaterales para la selección de blancos cibernética.³⁹ Aplicar fórmulas cinéticas sería problemático porque el ciberespacio existe tanto al nivel físico como lógico.

A pesar de estos retos singulares a la localización de blancos en el ciberespacio, la JP 3-60 ofrece un marco doctrinal suficiente para el planificador militar de operaciones cibernéticas.⁴⁰ Sin embargo, hay camino por recorrer y aclaración con respecto a las operaciones cibernéticas,

particularmente en los campos de cálculos de daños colaterales y evaluación de daños ocasionados por la batalla.⁴¹

Recomendaciones

Las mejoras a la doctrina existente de selección de blancos deben comenzar con una declaración en la próxima edición de la JP 3-60 que los conceptos básicos descritos en la publicación aplican a la selección de blancos en el recién reconocido ámbito cibernético. Dicha aseveración tendría el doble propósito de reconocer la importancia y singularidad de las operaciones militares en el ciberespacio y afirmar la universalidad de los principios de selección de blancos en combate de la publicación.

Tal como se mencionó anteriormente, la JP 3-60 debe ofrecer una reseña de cómo llevar a cabo un cálculo de los daños colaterales y la evaluación de daños ocasionados por el combate en el ciberespacio, quizás incluir tácticas, técnicas y procedimientos para identificar otros sitios de *Internet* hostiles y civiles ubicados en un servidor o rastrear posibles efectos de segundo y tercer orden y su probable ubicación geográfica. En realidad, en vista de que la mayoría de las operaciones cibernéticas ofensivas no ocasionarían daños colaterales, la JP 3-60 debe describir la metodología para definir *efectos* colaterales en el ciberespacio distinguiendo entre efectos y daños en el ciberespacio. Esa distinción debe usar el “daño cinético” (destrucción física o degradación ocasionada por una operación cibernética) como el criterio determinante. Cualquier operación cibernética que no ocasione destrucción física solamente produciría “efectos”. Los planificadores recopilarían las evaluaciones de daños ocasionados por el combate solamente para acciones que ocasionen daño físico a los blancos seleccionados y a los sistemas no seleccionados como blancos y medirían los efectos colaterales al igual que lo hacen para otras operaciones cibernéticas.

Una JP 3-60 actualizada debe incluir una sección breve sobre la complejidad del ámbito cibernético, utilizando las secciones del AFDD 3-12, “Comprendiendo el Ciberespacio” y “Entorno Operacional”, como una plantilla excelente.⁴² Una discusión de ese tipo le permitiría al planificador conjunto a reconocer las consideraciones singulares adicionales y la selección de blancos en periodos de tiempo específicos en y a través del ciberespacio.

Además, la siguiente versión del JP 3-60 debe prestar suma atención a las diferencias entre selección de blancos cibernética ofensiva y defensiva—específicamente el nivel de atribución necesario para la identificación positiva de un blanco cibernético. Para las operaciones cibernéticas de ofensiva (por ejemplo, CAN), la atribución de una red de computadora, sitio en *Internet*, individuo o infraestructura debe aproximarse a una certeza completa (una verdadera representación de la identificación positiva) de manera que cumpla con el principio de discriminación de las leyes de guerra. La aplicación del principio de auto defensa al ciberespacio le permite mayor flexibilidad al planificador conjunto, contando con la meta de repeler un ataque o ataque inminente contra sistemas de computadoras de aliados. El curso de acción recomendado para la defensa cibernética incluiría implementar una escala de atribución del adversario mediante la cual el nivel de confianza es acorde con el nivel de daño anticipado o efectos producidos por la respuesta. En un extremo de la escala, una respuesta cuyo alcance, duración e intensidad probablemente causará daño cinético significativo exigiría una certeza de atribución casi completa. En el otro extremo de la escala, una acción administrativa de auto defensa puramente técnica—quizás automatizada—que en realidad no llegue al uso de la fuerza no exigiría atribución. Esas “contramedidas” cibernéticas incluyen detectar, poner en cuarentena y eliminar un virus o sencillamente bloquear el tráfico malicioso e interrumpir las conexiones entre las computadoras que atacan y las que están siendo atacadas.

Por último, una JP 3-60 actualizada debe introducir conceptos sobre el *centro de gravedad cibernético de un adversario* y un *área ciberespacial de operaciones conjuntas*. La presencia cibernética de un adversario consta de computadoras, sistemas de informática, *hardware*, personas en línea, y de-

más, que puede que estén separadas geográficamente de su centro de gravedad físico. Una vez que los planificadores identifican el centro de gravedad cibernético (un punto crítico—una fuente de poder para las operaciones cibernéticas del adversario), lo pueden atacar. El comandante de la fuerza de tarea conjunta establecería las fronteras físicas y lógicas de un área de operaciones cibernéticas conjuntas y especificar las ROE de ataque para esa área. Dividir el ciberespacio de esta manera minimiza el potencial de daños colaterales y efectos en cascada.

En resumen, la JP 3-60 le ofrece al guerrero de guerra cibernética conjunta suficientes pautas para la selección de blancos en el ámbito cibernético. Sin embargo, con una ligera modificación y la incorporación de pautas específicas al ámbito, la publicación se tornaría aún más útil para los ciber guerreros. □

Notas

1. Wesley R. Andruess, “What U.S. Cyber Command Must Do” (Lo que el Comando Cibernético de EE.UU. debe hacer), *Joint Force Quarterly* 59 (4th Quarter 2010): 117, http://www.ndu.edu/press/lib/images/jfq-59/JFQ59_115-120_Andruess.pdf.

2. Tom Gjelten, “Extending the Law of War to Cyberspace” (Extendiendo el derecho de guerra al ciberespacio), National Public Radio Online, 22 de septiembre de 2010, consultado el 4 de octubre de 2010, <http://www.npr.org/templates/story/story.php?storyId=130023318>. Para fines de este artículo, *cinético* significa acciones físicas relacionadas tradicionalmente con el combate militar.

3. *DOD Directive* (DODD) (Directriz del DOD) 2311.01E, *DOD Law of War Program (Programa del DOD sobre el Derecho de Guerra)*, 9 de mayo de 2006 (incorporación del cambio 1, 15 de noviembre de 2010), 2, <http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf>.

4. En este artículo se emplea el término *principios* (1) dentro del contexto de selección de blancos para describir las creencias principales, mejores prácticas aceptadas y la filosofía militar para producir efectos operacionales y (2) dentro del contexto legal para describir los principios básicos de la ley. Sintetizados en publicaciones conjuntas, estos significados se dividen para destacar ciertas diferencias entre la acción militar cinética tradicional y posibles operaciones cibernéticas.

5. Joint Publication (Publicación Conjunta) (JP) 3-60, *Joint Targeting* (Selección de Blancos Conjunta), 13 de abril de 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf.

6. JP 1, *Doctrine for the Armed Forces of the United States* (Doctrina para las Fuerzas Armadas de Estados Unidos), 2 de mayo de 2007 (incorporación del cambio 1, 20 de marzo de 2009), I-1, I-21, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

7. El derecho de la guerra es “una rama del derecho internacional público, y consta de un conjunto de reglas y principios observados por las naciones civilizadas para la regulación de asuntos inherentes a, o secundarios a, la conducción de una guerra pública”. *Black’s Law Dictionary* (Diccionario de Derecho de Law), 6th ed. (St. Paul, MN: West Publishing, 1990), 1583.

8. Conferencias Internacionales (La Haya), *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land* (Convención IV de la Haya relativa a las leyes y costumbres de la guerra terrestre y su anexo: Regulaciones con respecto a las leyes y costumbres de la guerra terrestre), 18 de octubre de 1907, <http://www.icrc.org/ihl.nsf/full/195>. De aquí en adelante La Haya IV. Consultar también *Hague Convention (III) Relative to the Opening of Hostilities* (Convención III de la Haya relativa a la apertura de hostilidades), 18 de octubre de 1907, <http://www.icrc.org/ihl.nsf/FULL/190?OpenDocument>; *Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land* (Convención V de la Haya relativa a los derechos y deberes de las potencias neutrales y personas en caso de una guerra terrestre), 18 de octubre de 1907, <http://www.icrc.org/ihl.nsf/FULL/200>; y Geneva Conventions I–IV (Convenciones I-IV de Ginebra), 12 de agosto de 1949, International Committee of the Red Cross (Comité Internacional de la Cruz Roja), <http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp>.

9. Charter of the United Nations, Article 2(4) (Carta de las Naciones Unidas, Artículo 2(4)), 26 de junio de 1945, <http://www.un.org/en/documents/charter/chapter1.shtml>.

10. La Haya IV, Artículo 23(g).

11. La Haya IV, Artículo 23(e).

12. United Nations General Assembly Resolution 2444 (XXIII) (Resolución 2444 (XXIII) (de la Asamblea General de las Naciones Unidas), 19 de diciembre de 1968, según se menciona en International Committee of the Red Cross (Comité Internacional de la Cruz Roja), *Weapons That May Cause Unnecessary Suffering or Have Indiscriminate Effects: Report on the Work of Experts* (Armas que pueden causar sufrimiento innecesario o que tengan efectos indiscriminados: Informe sobre la labor

de expertos) (Ginebra, Suiza: Comité Internacional de la Cruz Roja, 1973), 13, http://www.loc.gov/rr/frd/Military_Law/pdf/RC-Weapons.pdf.

13. Consultar Ginebra IV, Artículos 4 y 27.

14. Judge Advocate General's School (Escuela de Auditores Generales), *Air Force Operations and the Law: A Guide for Air, Space, and Cyber Forces* (Las operaciones de la Fuerza Aérea y la Ley: Una guía para las Fuerzas Aéreas, Espaciales y Ciberespaciales), 2nd ed. (Maxwell AFB, AL: Judge Advocate General's School, 2009), 21, <http://www.afjag.af.mil/shared/media/document/AFD-100510-059.pdf>. Consultar la introducción a La Haya IV: "Los habitantes y los beligerantes permanecen bajo la protección y la regla de los principios de derecho de las naciones, como resultado de los usos establecidos entre los pueblos civilizados, del derecho de la humanidad y los mandatos de la conciencia pública".

15. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Diccionario de Términos Militares y Afines del Depto. de Defensa), 8 de noviembre de 2010 (según enmendado hasta el 15 de mayo de 2011), 362, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

16. Consultar al Mayor Keith E. Puls, ed., *Law of War Handbook* (Manual sobre el derecho de guerra) (Charlottesville, VA: International and Operational Law Department, Judge Advocate General's Legal Center and School, US Army, 2005), 139-42, http://www.loc.gov/rr/frd/Military_Law/pdf/law-war-handbook-2005.pdf.

17. Air Force Doctrine Document (AFDD) 2-1.9, *Targeting*, 8 de junio de 2006, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-60.pdf>.

18. El ciberespacio es un ámbito global. Consultar la JP 1, *Doctrine for the Armed Forces of the United States*, GL-7; and Cheryl Pellerin, "Cyberspace Is the New Domain of Warfare" (El ciberespacio es el nuevo ámbito de la guerra), *U.S. Air Force AIM Points*, 18 de octubre de 2010, consultado el 20 de octubre de 2010, <http://aimpoints.hq.af.mil/display.cfm?id=41748&printer=no>.

19. Mayor Steve Smart, "Warfare in the Cyberspace Domain" (La guerra en el ámbito ciberespacial) (tesis, Escuela Superior de Comando y Estado Mayor, Base Aérea Maxwell, AL, 2010), 3. Esta es la nueva definición de "ámbito ciberespacial" propuesta por el autor. La caracterización del ciberespacio como un ámbito operacional es sensible y controversial. Consultar el documento "White House Guidance Regarding the Use of 'Domain' in Unclassified Documents and Public Statements" (Guía de la Casa Blanca relativa al uso de "ámbito" en documentos no clasificados y declaraciones públicas), 14 de marzo de 2011. (FOUO)

20. Christina Mackenzie, "Do No Harm" (No hacer daño), *Aviation Week: Defense Technology International—Cyber War Issue*, Septiembre 2010, 37.

21. *Ibid.*

22. Michael Dumiak, "Casus Belli," *Aviation Week: Defense Technology International—Cyber War Issue*, Septiembre 2010, 31.

23. El subsecretario de la defensa para políticas y el presidente del Estado Mayor Conjunto revisarán la política y documentos de doctrina de las IO para reflejar la integración dirigida de las IO en las operaciones militares y alejadas de un enfoque en sus capacidades básicas. Este cambio marca un paso significativo hacia el alineamiento de las operaciones cibernéticas. Consultar memorándum de Robert Gates, secretario de la defensa, asunto: La comunicación estratégica y las operaciones de información en el DOD, 25 de enero de 2011, <http://www.carlisle.army.mil/dime/documents/Strategic%20Communication%20&%20IO%20Memo%2025%20Jan2011.pdf>.

24. JP 3-13, *Information Operations* (Operaciones de información), 13 de febrero de 2006, I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. La nueva definición de las IO es "el empleo integrado, durante las operaciones militares, de capacidades relacionadas con la información conjuntamente con otras líneas de operación para influenciar, interrumpir, corromper o usurpar la toma de decisiones de los adversarios y posibles adversarios a la vez que protegemos las nuestras". Ver Gates, memorándum 2.

25. JP 3-13, *Information Operations*, II-1.

26. Consultar JP 3-13.1, *Electronic Warfare* (Guerra electrónica), 25 de enero de 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf; y JP 3-13.2, *Psychological Operations* (Operaciones psicológicas), 7 de enero de 2010, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_2.pdf.

27. Esto no es para sugerir que el DOD no ofrece guías cibernéticas sino para destacar que hay muy pocas pautas para el guerrero. Consultar DODD 3600.01, *Information Operations (IO)* (Operaciones de información) 14 de agosto de 2006, <http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf>; and DODD O-8530.1, *Computer Network Defense (CND)*, 8 de enero de 2001.

28. AFDD 3-12, *Cyberspace Operations* (Operaciones ciberespaciales), 15 de Julio de 2010, 2, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>.

29. *Ibid.*, 16-20, 22-28.

30. Consultar AFDD 3-12, *Cyberspace Operations*.

31. El Comando Ciberespacial de EE.UU. está desempeñando varios roles y misiones en el ámbito cibernético y está creando una “visión unificada”. Mark V. Schanz, “Cyber Command Working Out Roles and Relationships” (Comando Ciberespacial resolviendo roles y relaciones), Daily Report, *airforce-magazine.com*, 21 de octubre de 2010, <http://www.airforce-magazine.com/DRArchive/Pages/default.aspx>. La 460ª Ala Espacial en la Base Aérea Buckley, Colorado, completó su primer ejercicio enfocándose exclusivamente en asuntos cibernéticos. Sgto. 1º J. LaVoie, “A First-of-Its-Kind Cyber Exercise” (El primer ejercicio cibernético en su clase), Daily Report, *airforce-magazine.com*, 29 de octubre de 2010, <http://www.airforce-magazine.com/DRArchive/Pages/default.aspx>.

32. JP 3-60, *Joint Targeting*, II-3.

33. Ibid.

34. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Ciberdisuasión y ciberguerra) (Santa Monica, CA: RAND Corporation, 2009), 11, http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

35. Consultar Timothy L. Thomas, *Cyber Silhouettes* (Siluetas cibernéticas) (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), 19.

36. JP 3-60, *Joint Targeting*, III-2.

37. Ibid., I-2.

38. Hay un debate de política en curso entre los profesionales cibernéticos y los líderes gubernamentales acerca de la necesidad de la identificación positiva para todas las operaciones cibernéticas y su factibilidad durante respuestas en casos de crisis

39. Consultar Comando de Fuerzas Conjuntas de Estados Unidos, *Joint Fires and Targeting Handbook* (Manual de fuego y selección conjunta de blancos) (Suffolk, VA: Joint Warfighting Center, Joint Doctrine; Norfolk, VA: Joint Capability Development, Joint Integrated Fires, 19 October 2007), http://www.dtic.mil/doctrine/doctrine/jwfc/jntfiretar_hdbk.pdf.

40. Mayor Kevin Beeker (acting J2T, US Cyber Command) y Sgto 1º Dustin Dargis (US Cyber Command), entrevistas con el autor, 2-4 de noviembre de 2010.

41. Ibid.

42. AFDD 3-12, *Cyberspace Operations*, 2-5.



El Mayor Steven J. Smart, USAF, (AA, Wentworth Military Academy Junior College; BS, John Brown University; MA, Air University; JD, Gonzaga University School of Law) es jefe de comunicaciones estratégicas, Oficina del Auditor General, Cuartel General de la Fuerza Aérea de Estados Unidos, Pentágono. Anteriormente se desempeñó en calidad de jefe de selección de blancos y derecho operacional en el Comando Cibernético de EE.UU. y sus organizaciones antecesoras, Comando Componente Funcional Conjunto-Guerra en la Red/Fuerza de Tarea Conjunta en la Red de Operaciones Global donde asesoró al comandante y a la Fuerza de Tarea Interinstitucional Conjunta sobre el derecho de guerra, reglas de enfrentamiento y derecho internacional durante la planificación de las operaciones militares en el ciberespacio. Fue el primer asesor jurídico para los equipos de selección de blancos y ataque cibernético, células de planificación de contingencia y en casos de crisis y para los planificadores de respuestas cibernéticas. Durante su carrera el Mayor Smart se ha desempeñado en calidad de fiscal militar y abogado de defensa al igual que abogado en derecho de suministros y ambiental. Además, desempeñó una función de liderazgo como vice auditor general. El Mayor Smart egresó en el 2011 de la Escuela Superior de Comando y Estado Mayor donde obtuvo el premio de investigación *Lt Gen Michael Hayden* por su contribución en el avance de las operaciones de información, inclusive influencia, guerra electrónica y operaciones de guerra en la red.

Profesionales Cibernéticos en las Fuerzas Armadas y en la Industria—Asociación en Defensa de la Nación

Conversación entre la General de División Suzanne Vautrinot, USAF, Comandante, Veinticuatroava Fuerza Aérea, y el Sr. Charles Beard, Director de Información, Science Applications International Corporation

TRANSCRITO Y EDITADO POR EL CAPITÁN JEFFREY A. MARTÍNEZ, USAF,
Y EL CAPITÁN MATTHEW R. KAYSER, USAF

UN DEBATE ESTRATÉGICO sobre cibernética ya no es un diálogo académico, y la tecnología asociada ya no es el dominio de los laboratorios de desarrollo de la industria o del gobierno. La “defensa” en el dominio cibernético es un imperativo nacional; los retos cada vez más complejos fuerzan a los ejecutivos superiores de la industria y del gobierno a ampliar los esfuerzos de colaboración para tratar estos retos. Las corporaciones de todo el mundo están aprovechando el dominio cibernético para suministrar bienes y servicios de forma más rápida y económica mientras equilibran la necesidad de proteger la información personal que les confían los clientes. Igualmente, los comandantes militares se basan cada vez más en las capacidades ciberintegradas para el mando y el control, y generar efectos en el campo de batalla, tanto cinéticos como no cinéticos. La clave para el éxito de la misión es salvaguardar los datos críticos, mientras se permite un acceso inmediato sin intercepción ni manipulación.

El 7 de noviembre de 2012, dos de nuestros ciberlíderes superiores de nuestra nación, la General de División Suzanne Vautrinot, comandante de la Veinticuatroava Fuerza Aérea y de las Ciberfuerzas Aéreas, y el Sr. Charles Beard, director de información y vicepresidente superior de Science Applications International Corporation (SAIC) se reunieron para tener una conversación. Durante esa conversación, el Sr. Beard narró una travesía de sus esfuerzos para reducir la superficie de ciberataque de su compañía y crear un entorno corporativo resultante en una solución de tecnología de información de una sola empresa, y la General de División Vautrinot no solamente articuló similitudes en la misión de la Fuerza Aérea de defender el país en el ciberespacio sino que también se concentró en cómo tanto la Fuerza Aérea como la industria pueden aplicar las lecciones aprendidas de éxitos como la migración de SAIC a medida que siguen avanzando hacia una postura de ciberseguridad más homogénea.

Con su consentimiento, nos gustaría compartir un diálogo privado entre colegas reconocidos y mutuamente respetados y socios en este dominio dinámico. Además, entrelazadas en esta conversación están las contribuciones de cada una de las escuadras ciberespaciales operacionales de la Veinticuatroava Fuerza Aérea, que explican puntos de debate clave y resaltan los esfuerzos actuales para poner en operación y normalizar el dominio ciberespacial.

Vautrinot: No es sorprendente, sus esfuerzos tienen sentido, y existe una verdadera similitud de experiencia en esta área. Usted ha tomado lo que eran elementos significativamente diversos de una corporación y ha cambiado completamente la dinámica—primero desde el punto de vista organizativo y después tecnológicamente. Estoy interesado en qué cambios organizativos cree que fueron los más esenciales para ese éxito; me gustaría aprovechar esos cambios para nuestra responsabilidad compartida en este entorno global variable.

Beard: La responsabilidad compartida es algo correcto. Al observar la cibernética, reconocimos que el modelo del gobierno tenía que cambiar. Crecimos como 10.000 oficinas independientes, y aunque eso tiene sus ventajas desde un punto de vista de desarrollo de mercados y capacidad de respuesta del cliente, tiene sus desventajas desde un punto de vista de dirección de la tecnología de información y de la escala de una empresa. Necesitamos una agilidad estratégica para participar en múltiples mercados globales y en un entorno informático cada vez más hostil. El primer paso consistió en definir y estabilizar el entorno, y eso significó cambiar la manera de pensar sobre la tecnología de la información.

Vautrinot: En las fuerzas militares, los mandos importantes o las organizaciones funcionales podrían considerarse de la misma manera—todas muy talentosas pero muy discretas . . . la descripción “cilindros de excelencia” se nos viene a la mente. Desde un punto de vista de las operaciones militares, esto tiene sentido, pero presenta retos al tratar las amenazas y el riesgo desde el punto de vista del ciberespacio. Como la tecnología de información y las comunicaciones crecieron de forma descentralizada, existe una inercia aparente para conservar ese método descentralizado. No obstante, usted ha demostrado la necesidad de crear una solución de empresa para operar mejor lo que es ahora una ciberempresa.

Beard: El primer paso para nosotros fue establecer esa relación y asegurarnos de que teníamos un verdadero punto de vista de empresa acerca del entorno y empezamos a operarlo como un haber de la empresa—sin que importe cómo se originó. Como siguiente medida, empezamos a trabajar con el gobierno para hablar sobre la necesidad de compartir información sobre amenazas y mejorar nuestra postura respecto al ciberespacio. Nosotros [SAIC] operamos entornos de tecnología de información en nombre del gobierno. Tenemos información de clientes en nuestras redes, y asumimos la responsabilidad de su administración muy seriamente. No obstante, al mismo tiempo, somos una compañía que cotiza en bolsa y operamos de forma global. No pudimos simplemente adoptar un punto de vista centrado en EE.UU. sobre cómo íbamos a resolver este problema ya que la Fuerza Aérea tampoco podría adoptar dicha posición. Tuvimos que cambiar la referencia intelectual para muchas personas cuando nos referíamos al gobierno y lo que significaba realmente como corporación multinacional tratar este problema del ciberespacio.

Vautrinot: En los dominios aéreo y espacial, teníamos la ventaja de desarrollar sistemas exclusivos y a menudo superiores o especializados: transición de aviones de la quinta a la sexta generación y satélites de última tecnología . . . inherentemente únicos. Era siempre sobre sistemas militares. No obstante, el ciberespacio es un entorno interconectado global. Compartimos el mismo entorno artificial, y la industria utiliza esa “última tecnología”. Las fuerzas militares no pueden permitirse el lujo—técnica o financieramente—de responder de forma independiente. Necesitamos una responsabilidad compartida—industria, gobierno, organizaciones educativas, socios internacionales—para alterar el entorno para obtener una ventaja colectiva y responsabilizarnos mutuamente del éxito. En lenguaje militar, podemos cambiar el dominio para proporcionar libertad de movimiento a nuestros aliados a la vez que la negamos a nuestros adversarios. Todos estamos trabajando en el mismo espacio aunque quizás necesitemos calcular el riesgo y la respuesta a la misión de un modo un poco diferente.

Beard: Lo esencial es la gestión de los riesgos y las respuestas medidas. Vuelvo a mis días del Mando Aéreo Estratégico, donde operábamos en el dominio nuclear. Aunque la misión de disuasión estaba clara, la misión de ataque se entendía igualmente bien. La preparación para ambas estaba a la orden del día. A diferencia de los otros dominios dentro de las fuerzas armadas—tierra, aire, mar y espacio—la proyección de fuerzas y el control del dominio cibernético son muy difíciles. Estamos utilizando una infraestructura compartida de base global, y el adversario a menudo tiene una posición que es igual o mejor.

Vautrinot: Veo una dinámica global similar en nuestro apoyo a misiones de aviones pilotados por control remoto. Para garantizar la misión, teníamos que llevar a cabo una amplia investigación inicial para entender los diversos enlaces de Estados Unidos con el vuelo en el extranjero. El sistema estaba diseñado con aproximadamente 180 puntos de contacto, muchos de los cuales no están militarmente controlados, a través de diversas redes, incluidos sistemas extranjeros, lo que hacía que fuera crucial establecer relaciones con organizaciones y aliados comerciales. La seguridad y la garantía se convierten en una interdependencia tremenda, que también se puede ver en la industria.

Beard: En el dominio comercial, interdependencia equivale a continuidad de operaciones y gestión de riesgos. Hay una diferencia en la forma que consideramos la amenaza, pero la garantía de la misión para una compañía comercial es impulsada en gran medida por los mercados y geografías en las que opera y el tipo de operación que se está llevando a cabo. El hecho que esas operaciones se lleven a cabo en una infraestructura compartida a escala global es un contexto importante para ejecutivos de la corporación a fin de que entiendan al sopesar riesgos.

Vautrinot: Los comandantes que respaldamos han indicado un imperativo similar para el acceso ininterrumpido a datos de confianza y verificables. La garantía de la misión en el ciberdominio es tan básica para la misión que no podemos permitirnos el lujo de perder la capacidad de comunicación—es esencial para el mando y el control militares.

Beard: Exactamente. Una compañía puede disponer de las mayores capacidades del mundo, pero no puede operar en el dominio digital y si no puede sostener un acceso ininterrumpido a la infraestructura de energía y comunicaciones, es muy difícil tener un perfil de misión que sobreviva. Así pues, consideramos el mando y el control como muy parecidos en el contexto de las misiones militares y comerciales porque estamos tratando de llevar a cabo operaciones comerciales en todo el mundo. Si no puedo proporcionar acceso para disponer de unas comunicaciones limpias y una energía ininterrumpida, entonces se deteriora considerablemente la continuidad el negocio.

Vautrinot: A nivel de corporación, ustedes tenían que ir más allá de tener conciencia de lo que pasaba. Las personas tenían que apoyar, entender la codependencia y ver su ventaja para el individuo. Tener un debate a menor escala hace que el efecto sea tangible y el cambio aceptable. Un negocio con éxito puede aprovechar esto para mover la compañía en nuevos sentidos. ¿Fue la comprensión algo que estaba adaptado a cada individuo y a escala, o tuvo el liderazgo superior que impulsar la conciencia de la empresa a fin de cambiar la cultura de la organización?

Beard: En SAIC, tenemos suerte de disponer de personas en nuestra junta directiva que han recorrido los pasillos del gobierno y de la industria, que entienden que esta amenaza es real. Así pues, lo que empezamos a hacer fue trasladar ese riesgo al contexto de la empresa. Creo que lo que encontrará es que diversas industrias comerciales están más adelantadas en ese entendimiento, esa madurez. Ciertamente la industria de servicios financieros ha entendido esto durante muchos años. Disponen de comités de riesgo separados en sus juntas directivas, y es uno de los muchos riesgos que deben tener en cuenta. Tenemos otras industrias, como la energía, donde la conciencia va en aumento incluso más. Son testigos del cambio del vector de amenazas de una simple recopilación de inteligencia a la destrucción operacional, según se indicó en el caso de Saudi Aramco.¹ En la industria médica, una compañía podría pasarse una década y gas-

tar 10.000 millones de dólares de EE.UU. fabricando un producto o un medicamento nuevos, y ver cómo una copia exacta de ese producto se lanza al mercado en un país extranjero un año antes de recibir la aprobación de la Administración de Alimentos y Medicamentos (Food and Drug Administration) [FDA]. Toda su propiedad intelectual se ha esfumado, por lo que la corriente de ingresos anticipados por esa compañía para ese producto durante los 10 años siguientes se reduce significativamente. Los imperativos económicos se están convirtiendo en un peligro claro y presente para la economía nacional donde operan estas empresas, pero muchas compañías siguen sin entender las amenazas cibernéticas y sus posibles impactos, tanto físicos como económicos.

Vautrinot: Existe un reconocimiento similar referente a la dependencia cibernética. No obstante, no estoy seguro de que se conozca el nivel de dependencia, y nuestra capacidad para llevar cabo todas las misiones—volar, combatir y ganar en el aire, espacio y ciberespacio. Nuestro reto, a medida que avanzamos, es crear relaciones en todos los elementos de las misiones . . . el tejido operacional frente a los hilos de las misiones. A medida que ampliamos este enfoque, debemos saber cómo equilibrar estos esfuerzos operacionales con la capacidad de mantener y defender nuestras redes. Según la Veinticuatro Fuerza Aérea, la Escuadra de Comunicaciones de Combate 689 se especializa en mantener este equilibrio ampliando las capacidades cibernéticas al límite táctico en apoyo del combatiente mientras continúa proporcionando comunicaciones defendibles y de confianza en ese límite.²

Beard: El hecho de que el correo electrónico se envía a servidores fuera de las redes de su compañía y posiblemente de fronteras nacionales—quizás a países que tienen leyes de interceptación diferentes de las propias—es algo que el usuario fortuito simplemente no entiende. Hemos construido empresas completas que dependen del dominio cibernético, pero no entendemos realmente los retos de seguridad asociados con ese dominio. Resulta desalentador cuando se empieza a entender cuáles podrían ser los impactos, y esa es la razón por la que el liderazgo es tan crítico para sortear este reto, y la ampliación ilimitada de dependencia de la red.

Vautrinot: En el entorno del presupuesto actual, existe un factor de complicación: el compromiso de recursos esperado cierra realmente el espacio de diálogo y decisión antes de poder explorar opciones. La complejidad de esta transformación a nivel de empresa se convierte en su propia clase de inercia. Si la cibernética está actualmente desordenada, entonces estamos atrapados entre la “entropía” natural del dominio y la inercia de la decisión. ¿Luchó usted contra eso en la industria?

Beard: Recientemente oí a un abogado sugerir que los directores de la corporación no deben estar mejor informados sobre riesgos de ciberseguridad debido a que las leyes les protegen de cosas para los que no están formados. Creo que eso era una opinión falta de perspicacia. Creo que en el contexto de la industria comercial—por ejemplo, un banco, una compañía de servicios pública, una compañía de ciencias farmacéuticas o un contratista de defensa—la base de estas empresas es su reputación y confianza. Las juntas directivas de esas compañías, con prácticas de gestión de riesgo robustas, saben muy bien si están en una posición informada para adjudicar esos riesgos. Para nosotros, el riesgo cibernético puede ser el riesgo más dominante que creemos afrontar. No obstante, para un contratista de defensa, quizás el mayor riesgo al que nos estamos enfrentando es que tienen a personas en peligro. Una institución financiera puede enfrentarse a una crisis de liquidez. Una compañía farmacéutica puede preocuparse sobre lograr una aprobación de la FDA para cumplir con ciertos pronósticos de ventas y localizar las versiones falsificadas de productos que venden en todo el mundo. La cuestión es cómo está de bien articulado ese riesgo, y esta noción de que podemos simplemente construir una fortaleza alrededor del negocio con ciberdefensas estáticas es simplemente la versión digital de la Línea Maginot.

Vautrinot: De acuerdo, las defensas estáticas no dieron resultado en la SGM y no darán resultado en el entorno cibernético. Esa es la razón por la que en la Fuerza Aérea, nos hemos estado

concentrando en una postura defensiva proactiva. En vez de esperar hasta que un adversario penetre en nuestras redes para evaluar nuestras vulnerabilidades, hemos creado equipos especializados que investigan nuestras redes y buscan esas vulnerabilidades, preferiblemente antes de que sean explotadas. Nos concentramos en identificar y defender esas interconexiones que son esenciales para el éxito de la misión—el General Keith Alexander, comandante del Cibermando de EE.UU., llamaría a esta capacidad “reconocimiento/contrarreconocimiento”. Una faceta clave de este esfuerzo defensivo es identificar y concentrarse en una “lista de haberes defendidos” prioritarios del comandante, esas áreas críticas que deben poder operar mediante un entorno en contención o un ataque. Esto corresponde directamente a algo de lo que hablamos antes: unir nuestros esfuerzos a la misión de la operación. Podemos entrar en un entorno de redes y proporcionar al comandante que depende de ese sistema información sobre decisiones de forma puntual y precisa. Específicamente, ¿puede fiarse en el sistema de la red para lograr su misión con éxito?

Esta postura proactiva se ve reforzada por el vector de información y amenazas compartido entre la industria y el gobierno. Un ejemplo soberbio era la Ciberseguridad de Base Industrial de Defensa Voluntaria /Programa de Calidad de Información del Departamento de Defensa, un acuerdo en el que las compañías, incluidas muchas de las mayores corporaciones en este país, colaboró con el Departamento de Defensa (en la Fuerza Aérea, a través del Equipo de Respuesta de Emergencia Informática de la Fuerza Aérea bajo la Escuadra de Combate de Redes 67) y el Departamento de Seguridad Nacional para compartir información de amenazas sensible y por lo tanto mejorar la defensa ciberespacial colectiva.³

Beard: Lo que se está empezando a ver ahora en el lado comercial es la frustración de estar en una defensa estática. La economía básica de los ciberataques favorece actualmente al adversario así como los dispositivos explosivos improvisados favorecen a los insurgentes. Para contrarrestar ese modelo, nos hemos asociado con la industria y el gobierno para desarrollar plataformas de confianza que permiten defensas dinámicas a través de nuestros productos Cloudshield. De forma alternativa, algunas personas de los mercados comerciales creen que es hora de devolver los puñetazos. Este movimiento desde la perspectiva de las ciberoperaciones consiste en pasar de la defensa de redes informáticas al ataque de redes informáticas. Me preocupan realmente las compañías comerciales que emprenden un tipo de misión de ataque de redes informáticas, con consecuencias no intencionadas tanto para la agencia de ejecución de la ley como para otras agencias gubernamentales.

Vautrinot: Históricamente según la ley internacional, el concepto de ataque pertenecía al dominio de la nación-estado. No obstante, las fronteras geográficas ya no demarcan actores a la ofensiva; por ejemplo, hemos visto compañías que venden servicios que dicen responder a las intrusiones cibernéticas enviando comandos o desviando tráfico malicioso. La naturaleza cibernética es que las compañías pueden tener capacidad de llegar mucho más lejos. Al hacer eso, disputarán con la ley nacional así como con los estatutos donde están operando o causando efectos. Desgraciadamente, las políticas nacionales e internacionales actuales no han seguido el ritmo de avance en las capacidades cibernéticas; por lo tanto, existen pretextos y lagunas completas en el gobierno que pueden ser aprovechados por corporaciones audaces.

En la Fuerza Aérea, no estamos limitados simplemente por leyes nacionales sino también por política gubernamental. Por lo general, el Departamento de Seguridad Nacional es responsable de defender los haberes cibernéticos fuera de las redes del Departamento de Defensa, pero sea cual sea la organización que esté contemplando estas acciones, los problemas de atribuir definitivamente una intrusión a un atacante particular y las acciones de armonización del uso del espacio con otras entidades son particularmente difíciles. Eso resalta una vez más la necesidad de una estructura de reparto de información entre el gobierno y la industria que facilite la acción rápida a los eventos cibernéticos.

Los líderes superiores de la Fuerza Aérea son ciertamente conscientes de las vulnerabilidades de nuestros sistemas de redes, pero ahora hay un reconocimiento intenso de las oportunidades para permitir la defensa así como para facilitar el éxito de la misión. Un gran ejemplo ha sido nuestro trabajo con el Mando de Transporte y Mando de Movilidad Aérea de EE.UU. Sus dependencias no están limitadas al dominio .mil sino al .com y la capacidad para trabajar con los socios de la industria para asegurar un movimiento mundial. Como consecuencia, son muy conscientes, y el entendimiento hace que sean muy proactivos en términos de resolución. Sin embargo, en otros mandos, existe una resistencia y creencia de que sus redes son “privadas” o están separadas de la Internet global y por lo tanto son sus adversarios inherentes. En lo que respecta a sus oficinas independientes, ¿experimentó una variación similar?

Beard: Lo hicimos. Teníamos empleados, socios e incluso clientes que operaban en lo que creían que eran redes “cerradas”; por lo tanto, no sentían que tenían un problema. Simplemente no vieron la necesidad de añadir capas adicionales de protección o ejecución de políticas en sus actividades. Lo que llamaron burocracia es lo que llamamos garantía de misión en el contexto de ingeniería de sistemas.

Vautrinot: Claramente, una necesidad de unidad de esfuerzo y con ella una cadena clara de responsabilidad—mando y control. Ciertamente, ustedes estaban implementando una solución de empresa por razones adecuadas, y el campo de oficinas independientes se dio cuenta de la importancia. No obstante, hay resistencia a perder lo que algunos creen que es su autoactualización—su capacidad de control. ¿Qué les permitió a ustedes aunar esa resistencia natural en el campo e impulsar la implementación?

Beard: Diría que tres cosas. Una era el compromiso de liderazgo. Teníamos que tener la voluntad del liderazgo para decir, “Deseamos ir aquí”. En segundo lugar, empezamos a educar al liderazgo, a la gerencia y a grupos de empleados seleccionados. Eso era realmente importante para nosotros—aumentar la conciencia. Por último, teníamos que reflexionar el contexto de ciberseguridad. Necesitábamos entender qué es lo que realmente había que proteger y dónde estableceríamos la confianza. Los resultados de ese ejercicio cambiaron materialmente nuestra estrategia de defensa profunda.

Vautrinot: ¿Qué nivel de liderazgo fue necesario iniciar? En nuestro idioma vernáculo, serían los mandos importantes y las funciones clave que dicen, “de acuerdo, estamos todos de acuerdo. Reconocemos la amenaza, y todos vamos a movernos juntos en este sentido”. Después, sería nuestra responsabilidad ayudarles a entender la justificación para implementar o tomar medidas que puedan ser localmente restrictivas.

Beard: Correcto, no todo el mundo estaba de acuerdo. Se requirió un mandato a nivel de director ejecutivo/director de operaciones/director financiero combinado, y rompimos algún que otro cacharro.⁴ Aunque la gente entendió la decisión de liderazgo y la necesidad de ejecución de políticas y supervisión, seguían queriendo autonomía, así pues desarrollamos herramientas para proporcionar autonomía mientras se preserva la postura de seguridad. Eso se hizo en el contexto de productividad y dando a la gente lo que quería. Lo que no entendimos hace 20 años, cuando las operaciones en el dominio digital empezaron a evolucionar, era este asunto de riesgo cibernético. El asunto del riesgo ha asomado ahora la cabeza, y no podemos ignorarlo, tenemos un conflicto. Deseo cuidarle como usuario final, como cliente, pero tengo esta otra responsabilidad que puede o no puede entender o apreciar, y trataré de ayudar a explicarlo. No puedo explicarlo simplemente a todos los usuarios finales porque no tengo los ciclos para hacer esto porque entonces no estoy haciendo mi trabajo. Eso, es parte del balance.

Vautrinot: Usted está protegiendo la viabilidad a largo plazo de la entidad corporativa, de la misma forma que estamos protegiendo la viabilidad a largo plazo de la misión y nuestro apoyo a la nación. Tiene que haber cierta libertad de acción, en toda la empresa, para permitir esa protección.

Creo que en la industria también tiene un requisito que reportar, no la ciberseguridad per se, sino su viabilidad como entidad corporativa en el dominio de la ciberseguridad. Si tuviera un informe similar, anticipo que no recibiríamos una nota de aprobado. No obstante, nos hemos movido hacia una estructura donde hay una gestión de nivel de haberes y empresas, pero solamente en las redes .mil y .smil. Cada una de las redes del sistema de misiones se define así mismo por separado y está provista y administrada de forma independiente. En su modelo, habría un “general” que sería designado para controlar la gestión de haberes de todas las interconexiones de redes de la Fuerza Aérea, desde los aperitivos hasta el postre—precisamente lo que se tenía que hacer en la industria. Es ciertamente necesario, pero he aprendido que la viabilidad operacional en este entorno en contención requiere un cambio fundamental en los haberes que gestionaríamos centralmente—requiere detectores para habilitar la conciencia y la respuesta proactiva a las amenazas dentro de la red. El primer paso, disponer de la gestión de haberes, por sí mismo es insuficiente, pero ser capaz de detectarlo—para obtener esa conciencia situacional y permitir que su sistema reaccione de modo automático—es el paso siguiente. ¿Cómo enfocó los cambios de nivel de ingeniería?

Beard: Eso formó parte de la segunda travesía en este proceso—instrumentalizar y hacer todo el análisis de vulnerabilidad de empresas y los escaneos con esa referencia. Esto permite preparar un monitoreo continuo. La razón por la que es importante es lo que compone la tercera travesía: tal vez desee cambiar mi red basándome en la misión comercial, la inteligencia de amenazas accionable y la intención de seleccionar adversarios que estén activos.

Vautrinot: Es aquí donde las operaciones del ciberespacio pueden facilitar las operaciones de la misión o dar alternativas de la misión. No necesitamos mandar y controlar la misión, sino que necesitamos tener una visibilidad completa de lo que ocurre en el [ciber]espacio y poder ajustarlo en tiempo real para desbaratar la posición del adversario. Hace que el conjunto de problemas del adversario sea mucho más difícil a la vez que se conserva la efectividad de la misión.

Beard: Exactamente. Porque si los adversarios entienden mejor su red que usted, usted tiene problemas, y si su infraestructura informática es tan rígida que no puede hacer asignaciones dinámicas, se van a aprovechar de eso, y una vez más las ventajas económicas y operacionales pasan al adversario. Esta es la razón por la que pasamos al modelo de nube híbrida—porque nos dio la oportunidad a nivel de aplicación y datos para mover cargas de trabajo de un lado a otro. Ahora puedo tomar una carga de trabajo que ha operado históricamente en servidores específicos en un centro de datos específico y asignar dinámicamente la carga de trabajo a máquinas virtuales que operan en centros de datos virtuales que pueden tener características geográficas diferentes. La información puede estar dentro de mi centro de datos, pero puedo moverla a lugares diferentes.

Vautrinot: En esa estructura, por ejemplo, la atención médica de los empleados no posee datos médicos, y el departamento de finanzas no poseería datos financieros. Mover y dar acceso a los datos deseados dentro de la empresa es la clave, y cada ramal de la empresa usa esos datos en vez de controlarlos como un elemento segregado. El objetivo no debe ser controlar sino tener datos de confianza accesibles en cualquier momento y en cualquier lugar. Nuestro reto es crear un entorno que sea constantemente ágil.

Los “ahorros” de eficiencia de tecnología de información parecen ser un término un poco desacertado. Al hablar con AT&T, Microsoft y socios de la industria como usted, la inversión inicial para hacer ese cambio no es solo una inversión de cultura y liderazgo corporativos sino también una inversión de capital significativa. No solo para ahorrar dinero en la operación a largo plazo de la tecnología de inversión sino una inversión financiera en ciberseguridad. ¿Cómo decidió su corporación la dinámica de inversiones para determinar que la compañía tenía el imperativo de poder permitirse la ciberseguridad? ¿Cuál fue el alcance de esa evaluación y ese diálogo?

Beard: No tratamos de ahorrar dinero al inicio. Tratamos de conseguir la agilidad estratégica y lo que eso significaba para nosotros como corporación global. Sabíamos que necesitábamos agilidad a nivel de empresa. Así pues, al hacer esta inversión, empezó a darnos la capacidad de empezar a ser flexibles. Considere esto no solo como usar esta tecnología para operar compañías sino en el contexto de cómo virtualizar compañías y recombinarlas. De hecho, SAIC está llevando a cabo una actividad así en este momento, y es interesante observar cómo la tecnología de información es un habilitador en vez de un obstáculo en el camino.

Vautrinot: La cibernética en este contexto que estamos describiendo—es una misión, y usted no es viable sin esta misión. A pesar de nuestra situación económica nacional actual, tenemos que hacer la transición del diálogo desde la reducción de costos hasta la defensa imperativa y por lo tanto merecedora de una inversión desde un punto de vista de estrategia nacional.

Beard: Eliminamos la cibernética por separado desde un punto de vista del presupuesto y la tratamos como si fuera una inversión estratégica. Si considera la tecnología de inversión como un centro de costos, perderá la oportunidad. Con el paso de los años he aconsejado a una serie de compañías que consideraban objetivos de reducción de costos en tecnología de información como una forma de cumplir con un objetivo de costo corporativo, pero el secreto es que adquieren deudas que no se muestran como un pasivo sin fondos ni en el balance general ni en el registro de riesgos de la empresa.

Vautrinot: Asimismo, mi “deuda técnica” es la falta de automatización y detección, que estoy superando manualmente—que en efecto es una fuerza laboral enorme que no es sostenible ni apropiada en un entorno cibernético dinámico. Impulsa respuestas de reacción ante problemas y excluye el suministro detectores y soluciones automatizados.

Nuestros esfuerzos para pasar de una red dispersa administrada por la instalación a una sola red homogénea administrada centralmente permitirá el seguimiento de detección y automatización necesario para liberar recursos y operaciones de red robustas a la escala requerida para una industria global, como la suya, u operaciones militares. Hasta entonces, esto impulsa un gran costo final.

Beard: Todos sabemos que la postura reactiva es más costosa. No haríamos nunca eso con un esfuerzo de desarrollo de sistemas de armas—tratamos de diseñar ingeniería firme en el inicio. Es mucho más económico a largo plazo hacerlo en ese orden.

Vautrinot: Se supone que las cosas que vemos, puede al menos tratarse, pero, ¿qué ocurre con las incógnitas desconocidas?

Beard: Las incógnitas desconocidas son inaceptables. Para fines de la Ley de Sarbanes-Oxley, por ejemplo, estamos obligados a tener listos controles preventivos.⁵ Las incógnitas desconocidas obligan a pensar a la “izquierda del suceso”.⁶ Pero eso le lleva a la conclusión de que no puede proteger todo. Así pues, llevemos a cabo un diálogo comercial o un diálogo militar sobre los haberes—podrían ser haberes de datos—que deseamos proteger.

Vautrinot: Es eso a lo que me refería como lista de haberes defendidos pero a un nivel discreto en vez de a un nivel de empresa. Hemos trabajado individualmente con el Centro de Control de Transporte Aéreo de Aviones Cisterna así como uno de los muchos centros de operaciones aéreas para demostrar esta dinámica. Pero no podemos aplicarla a un nivel de empresa porque no podemos “ver” o controlar los haberes cibernéticos en la empresa.

Beard: En mi función, puedo recibir una llamada telefónica donde se me diga, “Tengo este problema urgente de seguridad de información; ven y ayúdame”. Y las dos primeras preguntas son, “¿Cuándo se le hizo saber de un requisito para proteger este haber?” y “¿Cuándo supo que tenía este problema?” Si no estaba en la lista de haberes defendidos, no hice nada de forma proactiva para protegerlo, y si se ha exfiltrado o manipulado, no me ocupé específicamente de asegurarme de que se saliera de los límites o de preservar su referencia. Así pues, si la lista de haberes defendidos es incompleta, es muy difícil para mí desarrollar e implementar una política de ciber-

seguridad para proteger y defender esos haberes. Es un deporte de equipo, y hay una responsabilidad compartida para garantizar la misión que es increíblemente dinámica. Si usted compra simplemente un aparato de seguridad, para cuando lo despliegue, estará pasado de moda. Así pues, tiene una amenaza asimétrica, y usted está tratando de responder con un proceso anticuado tradicional. Es contraproducente, razón por la cual estamos tratando de cambiar las reglas del juego.

Vautrinot: Por supuesto, esa es la razón por la que estamos construyendo una plataforma que pueda ajustarse constantemente. Si estuviera usando una comparación de operaciones espaciales, definiría la interfaz entre la carga útil y la plataforma. Eso significa que necesito poseer la plataforma y la empresa y que puede hacer el ajuste en tiempo real. Por ejemplo, según el Coronel Paul Welch, comandante de la Escuadra de Operaciones de Información 688, desarrollamos la Plataforma de Operaciones de Información para proporcionar una estructura acreditada de arquitectura abierta para el despliegue rápido de aplicaciones de terceros.⁷ Esta capacidad de intercambiar nuestras herramientas permite un despliegue acelerado de esas herramientas, que proporcionan operaciones dinámicas y de respuesta a las operaciones ciberespaciales de la Fuerza Aérea y del Departamento de Defensa. Esto proporciona flexibilidad—como un avión caza, que puede configurarse para una misión aire-tierra durante una salida y para una misión aire-aire durante la siguiente. La diferencia es que el avión caza se reconfigura en horas/días, mientras que en el espacio cibernético debe ser en segundos.

Beard: Digamos que mi sistema de detección de intrusión ha sido anulado y necesito algo nuevo. La base de software forma parte de una plataforma y no es negociable, por lo que la plataforma de hardware misma no cambia. Puedo desplegarlo ahora mismo. Es esta máquina encubierta con controles fuera de banda la que solamente vemos, pero puedo poner distintas cargas útiles en ella.⁸ Las oficinas independientes pueden hacer lo que necesitan hacer, pero la empresa puede seguir dominando la red en su nombre. Ese es el truco—mando y control a nivel de empresa con ejecución descentralizada, un entorno dinámico que da a la empresa agilidad y “confianza” basadas en una plataforma que es muy configurable y le permite mirar a la “izquierda del suceso”.

Vautrinot: La intención, a medida que seguimos refinando nuestras destrezas en este dominio, es pasar de la postura reactiva a la proactiva y presentar objetivos ágiles detectables a nuestros adversarios. Todos nosotros, ya seamos del gobierno o de la industria, tenemos que fiarnos: debemos usar el capital intelectual disponible y las tecnologías emergentes para proteger nuestra información y sistemas a fin de evitar que pasen a formar parte de una cadena expansiva maliciosa [costo de remedio global de 2011 de 388.000 millones de dólares de EE.UU.].⁹ La travesía cibernética de la nación es una responsabilidad compartida, y es personal—solamente a través de asociaciones de desarrollo podemos seguir defendiendo esta nación en el ciberespacio.

El enorme alcance de este dominio es difícil de entender: en los próximos 60 segundos, se enviarán 168.000.000 de correos electrónicos; se anunciarán 695.000 actualizaciones en Facebook; y se llevarán a cabo 690.000 búsquedas en Google.¹⁰ A medida que se siguen multiplicando las posibles oportunidades en este dominio, también lo hacen las vulnerabilidades. Aquellos de nosotros que estuvimos presentes en este debate salimos de la habitación no solo con un mayor entendimiento de los retos futuros en este dominio sino también con una mayor apreciación de los esfuerzos de colaboración que tienen lugar entre el gobierno y la industria para salvaguardar la información crítica en que se basan las corporaciones, los comandantes y el país. □

Notas

1. En uno de los actos más destructivos de sabotaje informático al escribir esto, el 15 de agosto de 2012, un virus borró datos del 75% de las computadoras corporativas de Saudi Aramco, mostrando una bandera de EE.UU. en llamas en lugar de información. Debido al ataque, la compañía se vio obligada a reemplazar decenas de miles de discos duros.

2. La misión de la Escuadra de Comunicaciones de Combate 689 es capacitar, desplegar y suministrar comunicaciones expedicionarias y especializadas, control de tráfico aéreo, y sistemas de aterrizaje para operaciones de socorro humanitarias y operaciones de combate dominantes—en cualquier momento, en cualquier lugar. Para estar al día con el entorno estratégico rápidamente variable, los comunicadores de combates se basan en gran medida en la industria para proporcionar tecnología comercial, lo que les permite ampliar, operar y defender las capacidades ciberespaciales en los lugares más austeros y de la manera más efectiva posible.

3. Asegurar la defensa de información y sistemas militares—a través de la defensa de redes informáticas y ataques de redes informáticas—es un reto diario. La Escuadra de Combate de Redes 67 ejecuta operaciones de redes de la Fuerza Aérea, defensa, ataque y explotación para crear efectos ciberespaciales integrados en nombre de la Veinticuatro Fuerza Aérea y de los mandos combatientes. La escuadra opera dentro de las autoridades actuales del Departamento de Defensa para proteger la información y los sistemas de la Fuerza Aérea y del Departamento de Defensa y para asegurar la libertad de maniobra en el ciberdominio. El 67 incluye los operadores en la red responsables de la operación diaria de las redes de la Fuerza Aérea. La amplia colaboración entre el personal de la escuadra y otras organizaciones gubernamentales y civiles asegura el reparto continuo de información de amenazas cibernéticas a través de entidades públicas y privadas.

4. Al igual que “un toro en una cacharrería” rompe cacharros. En este caso, la introducción de los procesos de ciberseguridad rompió los procesos comerciales normales.

5. La Ley de Sarbanes-Oxley, una propuesta de ley del congreso promulgada en 2002, también conocida en el Senado como Ley de Reforma de Contabilidad de Compañías Públicas y Protección de Inversores, y en la Cámara de Representantes como la Ley de Rendimiento de Cuentas y Responsabilidad Corporativa y de Auditoría. La propuesta de ley se promulgó debido a un número de escándalos corporativos y contables importantes, incluidos los de Enron y WorldCom.

6. El término a la *izquierda del suceso* se refiere a una línea cronológica en la que cada incidente se marca con un suceso. Las actividades a la “derecha del suceso” son respuestas reactivas al incidente; esas acciones a la “izquierda del suceso” son acciones proactivas en preparación para dichos incidentes.

7. La Escuadra de Operaciones de Información 688 muestra estas operaciones de información y capacidades de infraestructura de ingeniería de funcionamiento demostrado integradas en los dominios del aire, espacio y ciberespacio. La escuadra ha desarrollado un proceso innovador de desarrollo de herramientas rápido acompañado por un programa de adquisición rápido que refleja métodos de sistemas inmediatos, intermedios y de largo plazo. La estructura de innovación comprende el Mando de Materiales de la Fuerza Aérea (AFMC) en colaboración con el Mando Espacial de la Fuerza Aérea para establecer un centro de innovación cibernética a fin de proporcionar capacidades ciberespaciales económicas, como la Plataforma de Operaciones de Información, en el intervalo apropiado para respaldar al combatiente conjunto.

La 688 amplía las innovaciones logradas por el tema de investigación de interés, organizadas por el Coronel Welch, asociándose localmente con expertos científicos y tecnológicos del Laboratorio de Investigación de la Fuerza Aérea y uniéndose simultáneamente con sus contrincantes de adquisición como el Coronel Chris Kinne, de AFMC en San Antonio, para ampliar la autoridad de adquisición local delegada de la Oficina del Secretario de la Fuerza Aérea para Adquisiciones. Se requiere un diverso conjunto de conocimientos colocalizados para complementar los conocimientos expertos de desarrollo cibernético residentes. El Teniente Coronel Jim Smith lidera la presencia del Centro de Pruebas y Evaluaciones Operacionales de la Fuerza Aérea en esta nueva organización a fin de probar y verificar la efectividad de las capacidades propuestas en un entorno operacional.

8. El control fuera de los límites pasa datos de control en una conexión separada de los datos principales.

9. *Norton Cybercrime Report 2011 (Informe Norton de delitos cibernéticos)*, Symantec Corporation, 7 septiembre de 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

10. “60 Seconds—Things That Happen On Internet Every Sixty Seconds” (60 segundos-Cosas que ocurren en Internet cada sesenta segundos), GO-Gulf.com, 1 de junio de 2011, <http://www.go-gulf.com/blog/60-seconds/>.



La General de División Suzanne M. Vautrinot, USAF (USAFA; MS, Universidad de Southern California) es la comandante de la Veinticuatro Fuerza Aérea, de las Fuerza Aéreas Cibernéticas y de las Operaciones de Redes de la Fuerza Aérea, Base de la Fuerza Aérea de Lackland, Texas. Ella es responsable de la fuerza aérea numerada de componentes de la Fuerza Aérea que proporciona a los comandantes combatientes fuerzas cibernéticas adiestradas y listas que planifican y llevan a cabo operaciones ciberespaciales. La General dirige las actividades de tres escuadras cibernéticas operacionales—dos con sede en Lackland y otra en la Base de la Fuerza Aérea Robins, Georgia—así como el Centro de Operaciones 624 de Lackland. La General Vautrinot ha servido en varias asignaciones, incluidas ciberoperaciones, planes y política, seguridad estratégica, operaciones espaciales y trabajo de estado mayor. Ha estado al mando a nivel de escuadrón, grupo y escuadra, así como en el Servicio de Reclutamiento de la Fuerza Aérea. La General ha servido en el Estado Mayor Conjunto, en los estados mayores de comandancias importantes, y en la comandancia de la Fuerza Aérea. Antes de asumir su posición actual, era la directora de planes y política, Cybercomando de EE.UU., Fort George G. Meade, Maryland, y la asistente especial al vicejefe de estado mayor de la Fuerza Aérea de EE.UU., Washington, DC. Asociado de Seguridad Nacional en la Escuela de Gobierno John F. Kennedy, Universidad de Harvard, el General Vautrinot es una graduada distinguida de la Escuela de Oficiales de Escuadrones, Colegio de Mando y Estado Mayor Aéreo (con honores), Escuela de Oficiales de Estado Mayor Conjunto y Combinado y Colegio de la Guerra Aérea (correspondencia).



El Sr. Charles E. Beard Jr. (BS, Universidad Texas A&M; MBA, Universidad de Montana) es el vicepresidente superior y oficial de información jefe para Science Applications International Corporation (SAIC) y gerente general de la Unidad Comercial de Giberseguridad de SAIC. En esta función doble, ha liderado el SAIC para convertirse primero en su industria a fin de efectuar la transición de la empresa a una infraestructura de cálculo de nube y tratar los retos de seguridad y control inherentes en esa travesía. Él es secretario de la Junta Fiduciaria de Inova Health Care Services y presidente de la Junta de Calidad en Inova Mount Vernon Hospital. Antes de incorporarse a SAIC, el Sr. Beard fue director de la división Oliver Wyman de Marsh & McLennan. En esta función, proporcionó servicios de recomendaciones estratégicas con transacciones y reestructuraciones corporativas y desarrollando estrategias de tecnología de información para lograr objetivos de diseño comercial. También sirvió como vicepresidente superior de Mercados de Transporte e Industrial Globales en KPMG Consulting (después BearingPoint), liderando la estrategia y los servicios de operaciones de la compañía para clientes comerciales globales, incluidas GE, Honeywell, United Technologies y Southwest Airlines. Ha completado una educación continuada en la Escuela de Negocios de Harvard y MIT Sloan. El Sr. Beard es un orador destacado.

Fronteras Nuevas, Realidades Antiguas*

DR. EVERETT C. DOLMAN

LA GUERRA INMINENTE CON China se librará para controlar el espacio ultraterrestre (exterior). Aunque sus efectos repercutirán ampliamente, el conflicto en sí no será visible para aquellos que contemplen el cielo nocturno. No será televisada. La mayoría ni siquiera se percatará de que está ocurriendo. Puede que ya haya comenzado.

No obstante, este nuevo tipo de guerra no será tan diferente al punto que sea irreconocible. Los principios de guerra y la lógica de la competencia permanecen intactos como siempre. Solamente el contexto ha cambiado. Cuando se perciben a través de esta perspectiva, a través de los principios de teorías tradicionales realistas y geopolíticas que han sobrevivido milenios en sus formas básicas, la conclusión inevitable es que Estados Unidos y la República Popular China (en adelante RPC) están en camino hacia la guerra.

En este artículo se ofrece una interpretación del contexto geopolítico neoclásico que le da forma al posible conflicto entre EE.UU. y China, coloca esa discusión dentro de una teoría más amplia de estrategia, tácticas y guerra y evalúa el potencial para una Gran Muralla del siglo XXI en la órbita terrestre baja.

Geopolítica neoclásica

Hace casi 2.500 años, Tucídides anticipó la inevitabilidad de una guerra del Peloponeso desastrosa a causa del “surgimiento de poder de Atenas y el temor que ocasionó en Esparta”.¹ De hecho, cuando un orden internacional existente es retado por una potencia en surgimiento, la autoridad hegemónica predominante se ve obligada a responder. Esas condiciones son relativamente raras en la historia, pero cuando suceden, la guerra resultante no es para lograr modificaciones fronterizas o botines insignificantes, sino para lograr el liderazgo de un nuevo orden mundial. Es una gran guerra, una *guerra hegemónica*.² Este es el contexto en el cual el mundo existe ahora. La relativamente estable hegemonía global del dominio estadounidense desde 1945, acentuada por guerras limitadas y cambios en los balances de oposición, es directamente desafiada por el surgimiento de poder de la RPC—y el temor que está creando en EE.UU. es palpable. Esa teoría determinista es rebatida rápidamente por aquellos que consideran que sus implicaciones son aborrecibles. La inevitabilidad es una adivinación grosera y poco sutil. Solo porque algo siempre ha sucedido no significa que siempre sucederá. Lo contrario tampoco es cierto. Porque algo nunca ha sucedido no significa que no puede suceder. El paradigma realista de la política de poder *no tiene* que dominar. La narrativa cruelmente consistente de la historia *no necesita* repetirse eternamente. Nada es inevitable, refutan los idealistas. El mundo se puede hacer diferente, el mundo hoy es diferente.

El poder de la posibilidad es tentador, pero la fortaleza brusca de la probabilidad, para el encargado de tomar decisiones, por lo regular es dominante. El pasado eclipsa el futuro—y con el tiempo el cálculo de la probabilidad, combinado con el riesgo, es más convincente que las perogrulladas. Si un evento es *probable*, y su influencia es clara, su resultado perceptible, entonces las preparaciones tienen que hacerse para mitigar sus efectos. Si un evento *no es probable*, aún si su impacto es grave, las acciones necesarias para mitigarlo a menudo se postergan para el futuro—aunque esta forma de apuesta política tiende a exagerar los efectos nocivos del evento

*Fuente: Publicado anteriormente en nuestra revista *Strategic Studies Quarterly*, Spring 2012

cuando eventualmente haya sucedido. Sin embargo, si la *soberanía* del estado está en riesgo, indistintamente de cuán poco probable sea el evento, se tiene que tratar directamente. La lógica bien entendida—si no aceptada en todas partes—de los cálculos de la razón de ser está completamente de acuerdo con los dictámenes geopolíticos clásicos que datan, como mínimo, a sus linajes teóricos.

La resurrección de la geopolítica como un conjunto válido de teoría militar está en su apogeo. Al aplicar los principios y dictámenes de la geopolítica a la era actual con un enfoque en las actividades espaciales, espero contribuir a su reinstauración. El que la reflexión geopolítica clásica debe exigir resurrección significa que ha atravesado un periodo de desaprobación y decadencia, una historia que necesitará análisis adicional. Por ahora, es suficiente afirmar que la geopolítica se derrumbó por su propio peso, por el mal uso y abuso al que sus seguidores la sometieron al llevar sus preceptos menos justificables a sus extremos. Al igual que el neoliberalismo, el neo-realismo y el neo marxismo buscan regresar a teorías básicas para su inspiración y evitar las tergiversaciones y la mala aplicación de seguidores que a menudo tienen buenas intenciones pero que lógicamente están fuera de onda, de la misma manera la neo geopolítica busca reafirmar sus principios básicos y una explicación en cuanto su mal uso en la historia.

Para su poder explicativo, la geopolítica busca características físicas y espaciales geográficas o centradas en la tierra.³ La unidad de análisis es el estado. Su ubicación, tamaño, recursos y población se colocan en el contexto de la ideología política, los valores socio-culturales y la tecnología para evaluar las formas de guerra dominantes en un momento dado. A la manipulación de este conocimiento se le conoce como *geoestrategia*; una evaluación dominada por el estado de las bases de poder geoespaciales en los planes o estrategias para la ventaja continuada militar, económica, diplomática y socio-cultural.

La geopolítica como un conjunto unificado de teoría no fue evidente sino hasta fines del siglo XIV, pero su linaje legado está claro en retrospectiva. En la medida que los fuertes hacen lo que quieren y los débiles sufren lo que deben, tal como Tucídides hizo que los atenienses majestuosos le dijeran a los melianos neutrales en su célebre diálogo sobre el poder del estado y el orgullo, la política de la realidad (*realpolitik*) siempre se ha enfocado en manipular el balance de poder existente por su persuasión.⁴ Aunque está separado conceptualmente de la geopolítica, tanto en teoría como en práctica, las dos escuelas de pensamiento son lógicamente inseparables.

La geopolítica describe las fuentes—el qué—del poder del estado; la geoestrategia explica el cómo. Ninguna provee la razón esencial—el por qué. Eso requiere una perspectiva teórica más amplia. La que dominaba a los arquitectos del pensamiento geopolítico se agrupa debajo de la rúbrica de realismo.

Si el poder del estado, expresado en términos de capacidad para la violencia, es *ultima ratio* (la razón final) de las relaciones internacionales,⁵ entonces la teoría geopolítica es extremadamente útil. Tucídides y Maquiavelo percibieron que el interés personal del estado coincidía con el de la humanidad; una jerarquía de temor, interés y honor.⁶ El estado que no se protege a sí mismo será vencido; lo que no crece se marchitará y morirá. El Cardenal Richelieu lo resumió en la frase *raison d'état* (razón de ser).

En un entorno de relativa escasez, los intereses de los estados coinciden en parte y se puede anticipar un conflicto. Los líderes prudentes reconocen los puestos y capacidades geográficamente ventajosas que realzan el poder del estado e intentarán controlar esos puestos—o como *mínimo negarle el control de esos puestos a un opositor*—para garantizar la salud y crecimiento ininterrumpido del estado. Un estudio de esas capacidades, incorporado a un plan para una ventaja continuada, se le conoce como geoestrategia.

Por ejemplo, Alfred Thayer Mahan alegó que en la era moderna, para poder lograr más poder se necesitaba poseer una armada capaz de proyectar influencia globalmente.⁷ Ya era hora, reafirmó cerca de fines del siglo XIX, que Estados Unidos creara una fuerza marítima que igualara su influencia económica, se despojara de su capa de aislamiento y se apoderara del lugar que le

correspondía a la vanguardia de las naciones estados. Sin duda, Mahan era un nacionalista estadounidense pero sus teorías aplicaban a *cualquier* estado en una posición similar. Mucho poder conlleva a mucha responsabilidad, él razonó, y Estados Unidos estaba derogando sus obligaciones al no asumir su liderazgo.

Halford Mackinder, el primer verdadero geoestratega global, describió un choque cíclico de poderes terrestres y marítimos a lo largo de la historia, una perspectiva que coincide con otras teorías prominentes de rivalidades recurrentes tales como la interacción de tecnologías o capacidades de ofensiva o defensiva para la maniobra o masa que tienden a dominar el espacio de batalla en una era en particular. El poder marítimo, alegó Mackinder, en ascenso con el desarrollo de la navegación confiable después de 1500, para inicios del siglo XX estaba cediendo el dominio de la maniobra al poder terrestre de fuerzas en masa a medida que la tecnología del ferrocarril creó líneas internas de abastecimiento y comunicación relativamente rápidas y poco costosas.⁸

A medida que la tecnología evolucionó, los detalles de la teoría geoestratégica se transformaron en decisiones que se podían poner en práctica, pero la lógica esencial persistió. Hubo argumentos similares para el poder aéreo y de misiles, y en la actualidad están en boga para el poder espacial. Al analizar las ramificaciones de un método astro político (*astropolitik*), varios enunciados parecen ser fácilmente aparentes:⁹

- La geopolítica clásica ofrece las explicaciones realistas más duraderas para los cambios en el sistema internacional.
- Muchas teorías geopolíticas clásicas resultan fácilmente adaptables para el ámbito del espacio exterior.
- Estas teorías, hechas a la medida para el poder marítimo, ferroviario, aéreo y de misiles, se pueden considerar como segmentos de un proceso evolutivo. *El poder espacial es su heredero lógico y obvio.*
- *El terreno especial del espacio exterior dicta las tácticas y las estrategias* para el aprovechamiento eficaz de los recursos espaciales.
- Hoy el espacio es una base de poder nacional—*un despliegue óptimo de los recursos espaciales es esencial* en el campo de batalla terrestre actual y el futuro basado en el espacio.

¿EE.UU. y la RPC o EE.UU. versus la RPC?

A primera vista, pareciera que las fuerzas geopolíticas actualmente están en balance dinámico. Estados Unidos es el poder marítimo y aéreo abrumador, orientado hacia la ofensiva y favoreciendo la maniobra y el ataque de precisión para la ventaja en la guerra. La RPC es potencialmente la potencia terrestre más grande que el mundo haya conocido, establecida defensivamente y dependiendo de masas de infantería como su fuerza principal. Ninguna tiene una ventaja significativamente global en relación a la otra. No hay ningún escenario a corto plazo verosímil en el que Estados Unidos pudiese invadir y sostener una ocupación del continente chino. Asimismo, Estados Unidos está actualmente inmune a cualquier invasión y ocupación por las fuerzas chinas. La soberanía de ninguno de los estados parece estar en duda a causa de acciones por el otro. Al nivel de gran estrategia, ni la maniobra ni la masa, ofensiva o defensiva tienen una ventaja transformacional. Desde este punto de vista, la guerra, aunque sea inevitable, no es inminente.

Teorías de conflicto menos venerables y la cooperación son más favorables hacia la paz a largo plazo.¹⁰ Económicamente, EE.UU. y la RPC están estrechamente atados. Los mercados chinos se están abriendo y la productividad en las fábricas de la RPC le ha permitido a Estados Unidos pasar a una economía posindustrial. El comercio está aumentado sustancialmente, y gran parte

de la deuda externa de Estados Unidos está en manos de China, al punto que a ninguno de los dos estados les conviene económicamente entrar en un conflicto que rompa (o tan solo debilite) esos lazos. Cultural e históricamente, los chinos y los estadounidenses se inclinan hacia una admiración y respeto mutuo. A pesar de las diferencias políticas entre el comunismo chino y el capitalismo democrático liberal occidental, las conexiones humanas y el acercamiento de los gobiernos son valorados por ambos lados. Un reconocimiento de la innovación tecnológica estadounidense y de la mano de obra y la ética espiritual china imbuye la relación que aún se está desarrollando. Ambos lados parecen estar dispuestos a tener relaciones diplomáticas y sostener un sistema mundial en el que cada nación estado tiene su lugar y su independencia.

Pareciera que en cada esfera, menos una, ambas potencias están esforzándose por lograr la paz. En cada esfera de competencia, con una excepción, hay lugar para la negociación y resultados mutuamente beneficiosos. El único ámbito incompatible e inflexible es el espacio exterior.

Acción Occidental versus Sincronización Oriental

La perspectiva estratégica esencial que confunde la cooperación en el espacio es una paradoja. La mente occidental considera que la transparencia y la franqueza como el camino más certero hacia la paz. Cuando un estado puede vigilar eficazmente a otro, se mitiga el temor del ataque sorpresa y se minimiza la tendencia a sobreestimar las capacidades e intenciones de un posible opositor. Con la transparencia, el dilema de la seguridad es innecesario y la cooperación es posible.¹¹

Pero la transparencia, como medida para forjar la confianza, es un modo de pensar puramente occidental. Para un estratega oriental, la idea de que un opositor podría saber con precisión los puntos fuertes y débiles solamente invitan al ataque. La clave para la estabilidad en esta perspectiva es la incertidumbre—no saber cuán fuerte o débil es un opositor y nunca, bajo ninguna circunstancia, revelar las de uno. Mientras más certero el conocimiento, más hábil el plan compensatorio, más probable será su éxito.

La desconexión esencial entre el Oeste y el Este en la conducción de la guerra es la diferencia entre la acción y la sincronización.¹² El estratega occidental muy a menudo busca imponer el cambio mediante pasos positivos. Los análisis se enfocan en la reacción probable a actividades específicas, y evaluaciones de si más o menos fuerza es necesaria para lograr el cambio. El futuro está construido completamente a través del esfuerzo e interacción de la acción.

Para el estratega oriental, la manera correcta de librar la guerra es cuestión de *sincronización*. El balance de la fuerza no es un solo cálculo sino uno continuo. El poder es una función de capacidades, posición y estado de ánimo—de la misma manera que lo es en el oeste—pero también es el resultado de numerosas fuerzas inmutables y a menudo desconocidas. La estructura domina a la agencia. En lugar de obligar un cambio a través de acciones positivas, el estratega oriental espera el momento oportuno para atacar. De hecho, la analogía de la jardinería es fuerte en los escritos militares chinos. Indistintamente de cuánto esfuerzo uno coloca en cosechar, aprender la jardinería, preparar el terreno, atender las plantas, no hay ningún beneficio en cosechar demasiado temprano o demasiado tarde.

En mi propia interacción con estrategias y generales chinos, las anécdotas confirman esas tendencias. Cuando se les propone que su ventaja radica en la planificación a largo plazo, esos funcionarios posiblemente se rían entre dientes. “Yo no sé qué va a suceder mañana”, él o ella responderá, “¿Cómo puedo saber lo que sucederá en años o en décadas? Lo que el estratega oriental hace es estudiar, prepararse y esperar. A través del estudio y la reflexión cuidadosa, el estratega aprende acerca de las fuerzas del opositor y las suyas, al igual que el terreno, tecnologías y contextos socio-políticos que cambian con el tiempo. Mediante la preparación y el entre-

namiento, las fuerzas militares que el estratega requiere están disponibles cuando se necesitan. Aguardar el momento correcto para la acción, garantiza el éxito.

La arrogancia occidental y el hermetismo oriental, por lo tanto, dominan sus relaciones de seguridad. Cuando Douglas MacArthur expresó sus famosas palabras de que no hay sustituto para la victoria, él estaba afirmando un dictamen centrado en el **agente**.¹³ Su significado era claro. Quien prevalece en la guerra no necesita hacer excusas por la manera en que se libraron las batallas. La historia la escribe el victorioso. En cambio, cuando Sun Tzu expresó que la cúspide de la destreza es ganar sin pelear, él no se refirió a una estrategia pasiva o inactiva.¹⁴ Él afirmó que al seguir el modelo de estudiar, prepararse y esperar uno llega a un punto en que el resultado es obvio para todas las partes, y un opositor capaz escogerá negociar los mejores términos en lugar de luchar hacia una conclusión previsible y desastrosa.

El análisis geopolítico tiene la capacidad de aceptar la lógica de *ambos* oeste y occidente. En lugar de escoger uno en lugar del otro, el geoestratega los percibe holísticamente y busca una tercera manera que *una* a ambos sin disminuir el poder de uno o del otro.

La Estrategia y el Ámbito Espacial

Dentro de la estrategia militar hay categorías *operacionales* de violencia o fuerza que están separadas por el ámbito.¹⁵ Esto es más que una categorización de economía o eficiencia de la fuerza. Es un reconocimiento que las estrategias para cada ámbito son singulares y constan de requerimientos individuales para la pericia táctica. Además, es el concepto operacional lo que une la lógica de la estrategia con la gramática de la táctica.

Un estrategia militar entiende los requerimientos de organizarse, adiestrarse y equiparse para la guerra. Este es el propósito singular del poder militar. Como tal, el estrategia militar superior prepara las estructuras de la fuerza en general y establece un plan general para su continua salud y pericia. Como función de esta práctica de organizar, resulta útil dividir los ámbitos de la guerra en tierra, mar y aire para poder asignar la autoridad de los servicios (para EE.UU., el ejército, la armada y las fuerzas aéreas respectivamente). Hoy, el espacio es reconocido ampliamente como un ámbito aparte, y algunas milicias estatales tienen servicios separados para él—por ejemplo, Fuerzas de Cohetes Rusos. En la medida que esos ámbitos son tan solo delineaciones convenientes se cree que la estrategia aplica igualmente a todos, aún cuando la pericia táctica puede que sea bastante diversa en ámbitos diferentes. Como tal, la manera como se dividen las fuerzas en tan solo una preferencia, subordinada a una teoría de guerra general. Para poder contar con una estrategia separada para cada ámbito, se deben percibir sus fines singulares. Contar con una estrategia para el espacio, o sea, una teoría de la guerra espacial, es necesario distinguir las funciones y misiones singulares del ámbito espacial. Si no hay nada singular, entonces la distinción no agrega ningún valor.

Además, los ámbitos o dominios singulares de la tierra, mar, aire y espacio (y quizás el ciberespacio) necesitan estar más separados física y conceptualmente, deben ser de valor complementario—de lo contrario estarán subordinados a otro ámbito—y anidados dentro del papel correcto que desempeña el poder militar. Típicamente, los ámbitos son separables por características físicas u operaciones de plataformas. En el caso anterior, el territorio de la tierra es el ámbito para el poder terrestre, los océanos y las vías fluviales definen el poder marítimo y las propiedades aerodinámicas o las características orbitales de los cielos definen el poder aéreo y espacial. En este último, si camina o se mueve en la tierra es poder terrestre y correctamente bajo el control del ejército; si flota u opera en el agua es responsabilidad de la armada; y si vuela a través del aire o el espacio es—para Estados Unidos—controlado correctamente por la fuerza aérea. No obstante, esto ocasiona una coincidencia problemática cuando se asigna la responsabilidad del ámbito. ¿Puede usar la armada aeronaves para patrullar los océanos? ¿A quién le pertenece y quién

opera un misil balístico lanzado desde un submarino que comienza su recorrido en el océano pero viaja a través del aire y el espacio y ataca una ciudad en la tierra? ¿Acaso la fuente u origen define la autoridad en el caso del submarino (poder marítimo), o debe ser el objetivo el que define esa autoridad (poder terrestre)? Si se lleva al extremo, todas las operaciones marítimas, aéreas y espaciales comienzan en la tierra; ¿deben las armadas y las fuerzas aéreas-espaciales participar exclusivamente en apoyo a las actividades para el ejército? Esto también crea más problemas de los que resuelve. Si discrimino según el objetivo, ¿estoy llevando a cabo una guerra económica cuando destruyo una fábrica, indistintamente de los medios? Si bombardeo una escuela con una aeronave, ¿estoy llevando a cabo una guerra educativa?¹⁶ Eso es absurdo. Lamentablemente, el modelo para la discriminación de poder ya se ha definido; al igual que la fuerza militar como un medio del poder estatal, la autoridad del ámbito se comprende mejor como una función de *propósito*. Cuando se define de esta manera, los enigmas mencionados arriba desaparecen.

La finalidad *militar* del poder terrestre es apoderarse y mantener el territorio. Esto se entiende como *control* y es la misión asignada correctamente a los ejércitos. La finalidad *militar* del poder marítimo es controlar el mar. Las armadas hacen eso. La finalidad *militar* del poder aéreo es controlar el aire. De la misma manera, la finalidad *militar* del poder espacial es controlar el espacio. Si seguimos el dictamen principal de la geopolítica clásica, *si el control no se puede lograr o sostener, entonces es vital que un posible adversario no pueda ni lograr ni sostener el control*. Esto se conoce como *disputa*. Por lo tanto, las fuerzas terrestres deben organizarse, entrenarse y equiparse para controlar y disputarse la tierra; las fuerzas navales los mares; las fuerzas aéreas el cielo y, fundamentalmente, si el espacio es un ámbito bélico aparte, entonces las fuerzas espaciales deben estar preparadas y aptas para controlar y disputarse el espacio.

El control provee de *usar* el ámbito para crear efectos. En otras palabras, lo que uno *hace* con el poder terrestre, marítimo, aéreo o espacial depende completamente de la capacidad para operar desde o a través de la tierra, mar, aire o espacio. En el caso del poder aéreo, la capacidad de bombardear, trasladar abastos o hacer observaciones con aeronaves requiere que uno pueda entrar en el aire y luego en el blanco. Sin embargo, al igual que con el poder militar, lograr el control de manera que el ámbito se pueda usar no significa necesariamente la aplicación constante y dominante de la aplicación de la fuerza militar a lo largo del ámbito. En un entorno *no impugnado*, el acceso se basa completamente en la capacidad de obtener y utilizar los recursos necesarios para moverse de un punto a otro y hasta qué punto se acatan las reglas legales que coordinan las operaciones en áreas congestionadas (por ejemplo, regímenes de control de vuelo en aeropuertos). Sin embargo, la presencia continua de un ámbito no impugnado se ha debido históricamente a la existencia de una capacidad de la milicia o fuerza policial que se mantiene en reserva para garantizar que se obedecen las reglas y que se castigue la inhibición no autorizada del movimiento en el ámbito. Este es el caso actual del área común global aérea y marítima. La Armada de EE.UU. es principalmente quien garantiza que las 12 millas de extensión actual de soberanía nacional en los océanos no se sobrepasen (como sucedió con sus acciones en el Golfo de Sidra en cuanto a Libia), o que estrechos vitales en las rutas marítimas comerciales no estén bloqueados (por ejemplo, los Estrechos de Hormuz) y que se evite o castigue la actividad criminal no estatal (tales como los esfuerzos en curso contra piratas somalíes en el Océano Índico). Sin embargo, sin la capacidad de aplicar la fuerza *sobre* y *en* los mares, para abordar e inspeccionar embarcaciones sospechosas o que violan las leyes, escoltar y defender pasajeros inocentes y más, la Armada de EE.UU. no puede defender o disuadir en los mares sin violar la soberanía de otros estados o depender de recursos no navales para la disuasión y el castigo.

En el espacio ningún estado aún ha intentado lograr el control general de un lugar perceptible, y las naciones capaces de operar en el espacio en su mayoría lo han hecho según las obligaciones jurídicas o de tratados. Este es el modelo que se siguió en el aire durante su desarrollo inicial (y probablemente con acceso al mar en algún momento en la prehistoria). Hasta la Primera Guerra Mundial no ocurrió la disputa del aire. El acceso sin restricciones era una función

de deseo, tecnología, aerodinámica, clima, leyes y dinero. Tal es el caso hoy con el espacio. Ningún estado aún ha actuado militarmente para disputar el uso del espacio por parte de otro estado (que sepamos). La zona geoestacionaria está regulada por un acuerdo internacional y hay varias leyes que limitan la colocación de armas de destrucción en masa en el espacio. Normas de registro y responsabilidad han sido creadas y ampliamente aceptadas, y los efectos disponibles desde naves espaciales y el uso del espacio están, por lo regular, disponibles para todos—sin embargo, la explotación del espacio aún es menos que óptima.¹⁷ Ningún equivalente a la Armada de EE.UU. está al acecho para cerciorarse que los estados parias *no* puedan extender su territorio soberano más allá de los límites de vuelo generalmente aceptados o para detener actividades ilícitas siempre y cuando ocurran. Las actividades militares ocurren para crear escombros y otros peligros a la navegación, pero no hay ningún equivalente a un barredor de minas para eliminar los desechos militares indeseables. Y si algún estado u organización *desease* disputar o controlar el espacio, negándole los frutos del mismo a otro estado, sencillamente no hay *defensa* contra una acción de esa índole—solo hay disuasión a través de la amenaza asimétrica de represalias centradas en tierra.

La *disputa* es la capacidad para bloquear o negar acceso a un ámbito. Fundamentalmente, la disputa no otorga la capacidad para *usar* un ámbito; solamente lo inhibe. Es por ello que para un estrategia militar, el control es un concepto vital. El control puede ser general o limitado a horas y lugares específicos, pero sin la capacidad de entrar a un ámbito y operar ahí, él o ella no puede utilizarlo para crear efectos. Por lo tanto, por *cada* ámbito militar, *el control es posible solamente desde dentro del ámbito*. Esto es obvio cuando se disputa el ámbito, pero también se debe ejercer en un ámbito no disputado cuando actividades ilícitas o perjudiciales ocurren en él.

Una extensión de la necesidad de controlar un ámbito para poder utilizarlo es el entendimiento de que para *mantener* el control un planificador militar debe poder disputarse las zonas litorales de aquellos ámbitos adyacentes al mismo. Por ejemplo, se requiere un ejército o una fuerza terrestre para lograr el control militar y luego hacer uso del territorio disputado. Este es el tan pregonado concepto de la necesidad de contar con botas en el suelo. En la medida que se necesite el control territorial, se requieren botas en el suelo (o ruedas, rieles, etc.). En la medida que se desee el control del aire sobre territorio enemigo para poder bombardear los blancos, las botas en territorio enemigo puede que sea irrelevante. Llamémosle a esto las alas en el dictamen aéreo y hacer otra para los remos en el agua. Para poder utilizar el ámbito, debo poder operar en él.

La fuerza terrestre que ocupa o controla un territorio no podrá maximizar el uso del ámbito si el espacio aéreo sobre ese territorio no está controlado por fuerzas amigas. Por lo tanto, la fuerza terrestre debe intentar bloquear el acceso a las fuerzas aéreas opositoras o aceptar el vuelo libre de aeronaves enemigas sobre sus posiciones. Lo último puede que sea una necesidad, si los medios para disputarse el aire no están disponibles, pero es una condición operacional indeseable. Por este motivo, las fuerzas terrestres por lo regular cuenta con artillería y misiles antiaéreos. Las fuerzas terrestres también erigen defensas costeras para evitar ataques e invasiones desde el mar. En vista de que la finalidad de estas acciones es disputarse los litorales del ámbito terrestre, están correctamente asignadas e integradas en las operaciones y la doctrina del ejército. Por su parte, las armadas mantienen fuerzas terrestres—infantería de marina y policía costera—para disputarse las playas y proteger los puertos. Las armadas también cuentan con capacidades antiaéreas significativas en sus buques y mantienen flotas de aeronaves para refutar los esfuerzos contra buques de los opositores. Las fuerzas aéreas también deben asegurar las bases y refutar los esfuerzos antiaéreos de los ejércitos y las armadas. De la misma manera, las fuerzas espaciales *deben* contar con la capacidad de negar *desde* el espacio armamento contra satélites basados en tierra, mar y aire.

Puede que haya ocasiones en las que un estado no necesite o desee disputarse o controlar un ámbito. Un estado sin litoral no verá la necesidad de crear una fuerza naval para controlar el

mar, y probablemente no adquirirá una capacidad especializada para disputarse el mar. La mayoría de los estados intentarán obtener capacidades para disputarse el aire, tales como los misiles avanzados de superficie a aire, pero muchos no podrán sufragar los recursos para controlar el aire. Sus estrategias militares serán creadas con un entendimiento que los efectos lanzados desde o a través del aire, tales como apoyo aéreo cercano o reabastecimiento aéreo, probablemente no estarán disponibles en un momento de conflicto o crisis.

Si el espacio es un ámbito militar, entonces debe seguir la misma lógica. Un estado que depende del apoyo militar desde el espacio—los efectos que logra al disponer de recursos en el espacio—debe planificar para lograr, como mínimo, control limitado o temporal del espacio en tiempos de conflicto. Y, como ya es obvio de la descripción anterior de ámbitos análogos, *el control es posible solamente desde dentro del ámbito*. Si el estado *no está dispuesto* a colocar armamento en el espacio, entonces no puede esperar a *garantizar* efectos desde el espacio cuando otro estado intente disputarse su posición. Su recurso lógico es deshacerse rápidamente del apoyo, mejora y habilitación espacial, y pasar a una estructura de fuerza militar pre especial. Entonces, debe dejar de gastar dinero de las adquisiciones, producción y personal en el espacio militar. Si es razonable sospechar que la milicia será obligada a combatir sin apoyo espacial garantizado, entonces debe entrenarse para ello. La milicia más eficaz en un entorno en que se le ha negado el espacio será aquella que no requiera en lo absoluto el uso del espacio. Desde luego, si una fuerza militar es ducha en combatir sin el espacio, ¿por qué debe gastar recursos escasos para organizarse, entrenarse y equiparse para combatir de otra manera? Para un comandante, sería el colmo de la locura depender de una capacidad que puede que esté o no disponible cuando se le necesite. Con el poder militar preparándose para combatir sin el espacio, el financiamiento del gobierno para continuar el apoyo espacial militar se debe reducir progresivamente y a la larga descontinuar. Sin una presencia militar que proteja los recursos espaciales frágiles y garantice el cumplimiento de tratados en el espacio, junto con reducciones drásticas en la industria espacial a medida que los contratos militares terminen, el desarrollo comercial del espacio será reducido drásticamente. Sería absolutamente prudente crear armamento anti espacial basado en tierra, mar y aire, de manera que un opositor no pueda usar libremente el espacio, pero gastar dinero y esfuerzos en una capacidad en el espacio que sería bueno poseer y que no se necesita para llevar a cabo las operaciones en tierra sería absurdo.

Siguiendo esta lógica, negarse a uno la capacidad de colocar una fuerza militar *en* el espacio es equivalente a desistir del *valor* militar (y quizás civil) del espacio.

Con certeza, el costo de armar el espacio eficazmente será inmenso. Es un costo que necesita asumirse si Estados Unidos, o cualquier otro estado, está decidido a contar con una estructura militar que dependa del apoyo y habilitación espacial para operar como lo hace hasta ahora, mucho más para el futuro. Y *tendrá* beneficios para la milicia que quizás no sean evidentes; por que ¿de dónde vendrá el dinero para esta capacidad de armamento espacial? No vendrá de los presupuestos escolares o de los programas de ayuda al extranjero. No vendrá a expensas de la reforma de cuidado de la salud o rescates financieros a las corporaciones. Vendrá a expensas de la capacidad de las aptitudes militares *convencionales* en tierra y en el mar y en el aire. Habrá menos portaaviones y aeronaves de combate y bombarderos más costosos. Si se despliega armamento espacial capaz de atacar la tierra, los relativamente lentos buques y aeronaves serán obsoletos conceptualmente e instantáneamente vulnerables a ese armamento. A medida que se obtiene dinero para los láseres espaciales y satélites cinéticos exóticos, los sistemas que estas armas espaciales tornen indefensas serán desechados. Más fondos vendrán del desarrollo y despliegue en curso de misiles balísticos y anti balísticos, a medida que la defensa *global* de misiles balísticos desde el espacio es más económica y práctica que sistemas exhaustivos basados en tierra y en el mar. Y, más importante aún, los fondos vendrán de las reducciones de personal, de tropas terrestres actualmente ocupando territorio extranjero. De esta manera, Estados Unidos conservará su capacidad de usar la fuerza para influenciar estados alrededor del mundo, pero atrofiará

su capacidad para ocupar su territorio y amenazar directamente su soberanía. La era de la hegemonía estadounidense será extendida, pero la posibilidad de un imperio global estadounidense será reducida.

Quizás. El futuro no está determinado o ni siquiera se puede determinar. Yo he alegado en otros lugares la viabilidad de controlar el espacio. En este escrito no agregaré a ese argumento. También he destacado que la teoría que estimula esas conclusiones es precisa y bien elaborada, pero el mundo real es demasiado complejo para reflejar la teoría. La voluntad política necesaria para armar el espacio y darle seguimiento con un régimen capaz de garantizar el desarrollo comercial y cooperativo del espacio aún no es evidente, y esa visión *astropolitik* puramente realista por lo tanto no es viable actualmente. Pero el apoyo para el bien común y colectivo que podría emanar de una fuerza espacial correctamente armada podría cambiar eso. Hay algunas posibles misiones para el armamento espacial que no le restan valor a su finalidad principal pero sí complementan la meta del control espacial que algún día podría ayudar en lograr la voluntad de pagar y usar ese armamento. El deseo de limpiar los escombros de las órbitas de gran tráfico podría hacerse teóricamente mediante láseres activados nuclearmente y basados en el espacio—buena práctica en atacar para sus operadores. El acceso garantizado al espacio por una fuerza de control espacial robusta podría preparar el camino para deshacerse de manera limpia y permanente de los desechos nucleares y tóxicos, ya que éstos se almacenan en tierra en la actualidad y podrían ser enviados al Sol. La generación de la energía solar basada en el espacio podría proveerle al mundo exhaustiva y económicamente con energía abundante que le restaría énfasis al valor y la autoridad de los estados productores de petróleo y básicamente cambiar el paisaje geopolítico de la Tierra. Estos escenarios son mucho más probables que se cristalicen con la vigilancia y protección provista por una potencia militar o policial basada en el espacio.

Para aquellos que se oponen a las armas en general, y en particular las espaciales, es un dilema aún más difícil. Las ramificaciones de la misión *actual* más crítica del Ejército, Armada e Infantería de Marina—pacificación, ocupación y control del territorio extranjero—son profundas. Con la reducción de las armas tradicionales para acomodar gastos espaciales más elevados, la capacidad de hacer esas tres misiones decaería significativamente. En un momento en que muchos aclaman *mayor* capacidad para pacificar y vigilar tierras extranjeras, en virtud de los despliegues sin fin de las fuerzas mantenedoras de paz estadounidenses alrededor del mundo, los defensores del armamento espacial tienen que abogar por la *reducción* de esas capacidades a favor de un sistema que no tendrá un potencial directo en hacerlo.

Por lo tanto, el argumento de que el despliegue unilateral del armamento espacial precipitaría una carrera armamentista desastrosa se deteriora aún más. Con certeza, el armamento espacial es ofensivo por naturaleza. Disuaden la violencia por la amenaza omnipresente de represalia precisa, medida e incontenible. Pero no ofrecen ninguna ventaja en la misión de ocupación territorial. Como tal, son mucho menos intimidantes al entorno internacional que cualquier otra combinación de armas convencionales utilizadas en su lugar. ¿Qué sería más amenazador para un estado opuesto a la hegemonía estadounidense: Una docena de láseres en el espacio con precisión milimétrica o (quizás por el mismo precio) una docena de divisiones de infantería amasadas en su frontera? Un estado que emplea la disuasión ofensiva mediante el uso de armamento espacial puede castigar a un estado transgresor, pero está en una posición pobre para retar la soberanía de ese estado. Es menos probable que un estado transgresor sucumba al dilema de seguridad si percibe que su supervivencia nacional no está en riesgo. Además, el gasto tremendo de armamento espacial impediría su uso indiscriminado. Con el tiempo, el mundo de estados soberanos podría reconocer que Estados Unidos no podría ni utilizaría el armamento espacial para amenazar la autodeterminación nacional de otro país. Estados Unidos aún desafiaría cualquier intento de intervenir militarmente en la política de otros, y restringiría gravemente su propia capacidad de hacer lo último. El uso acertado y no arbitrario de un espacio armado a

la larga podría considerarse como un positivo neto, una fuerza global eficaz que castiga actos criminales pero que no amenaza atacar de una manera imperialista.

Una Gran Muralla del Siglo XXI en el Espacio

Hace poco más de tres años, China le disparó con éxito a uno de sus propios satélites en el espacio.¹⁸ Esto fue extraordinariamente provocativo. Estados Unidos sencillamente no cuenta con ninguna defensa contra ese tipo de armamento, y la intención de la prueba anti satélite por parte de China era recordarle al mundo su debilidad. Además, su uso del MRBM (que la RPC produce en masa) para accionar el vehículo indica una posible capacidad de armamento anti satélite lo suficiente para atacar todo el inventario de EE.UU. de la órbita baja de la Tierra. Esfuerzos en curso para colocar interceptores de misiles basados en tierra en lugares estratégicos serían inútiles, indistintamente del despliegue, ya que éstos están diseñados para atacar misiles balísticos que se aproximan en la fase de vuelo media o terminal. El misil chino logra la altitud orbital pocos minutos después del lanzamiento, por lo tanto la única defensa posible contra él—que tendría la ventaja adicional de garantizar que cualquier escombros destructivo de un ataque exitoso aterrizaría en suelo chino—sería una red de satélites de misiles antibalísticos operando en la órbita de la Tierra.

Justamente esa capacidad anti misil basada en el espacio, imaginada hace años y técnicamente factible desde fines de la década de los ochenta, ha sido por mucho tiempo la solución óptima para los planificadores militares. Sin embargo, ese tipo de sistema ha sido postergado anualmente a causa de cálculos de costo elevado y temores de exhortar a otros estados a que diseñen armamento anti espacial. La última inquietud ha sido superada por los acontecimientos. Pero el problema del costo continúa.

Con la guerra global contra el terrorismo y despliegues terrestres importantes captando la mayor parte de la atención y del presupuesto, cambiar fondos de requerimientos operacionales inmediatos a seguridad a largo plazo no es fácil. La *coordinación* de la prueba anti satelital china coincide perfectamente con su percepción de que Estados Unidos no está en condiciones de responder con fuerza, y probablemente tienen razón.

La meta final de China parece ser hacer valer su supremacía regional y lograr un estatus **co-igual** (si no dominante) como una potencia global. El control del espacio es un paso crítico en esa dirección. Sin sus ojos y oídos en el espacio para proveer advertencia e inteligencia en tiempo real, Estados Unidos estaría en una posición terriblemente difícil si la RPC presionara militarmente a Taiwán. Para aquellos que alegan que China está igual de ansiosa por evitar una guerra dañina en el espacio al igual que cualquier otro estado que transita por el espacio, especialmente en vista de su integración cada vez mayor a la economía mundial y la dependencia en el comercio extranjero para su prosperidad continua; no descartan las capacidades de su liderazgo autoritario. Este es el mismo régimen que adopta las penurias de la pobreza cíclica inducida por el gobierno para librar a su población de la decadencia moral del lujo capitalista.

Al igual que con la famosa Gran Muralla que se extiende a lo largo del norte de China, construida con el doble propósito de impedir incursiones nómadas y crear una magnífica obra pública para legitimar el gobierno e inspirar a su población, una presencia militar significativa en la órbita baja de la Tierra tiene un valor paralelo para la RPC hoy. Su capacidad cada vez mayor en el espacio es extremadamente popular internamente (además de darle una mejor reputación a la capacidad de China de desarrollar productos y servicios de alta tecnología) y ayuda a disminuir la disconformidad interna al legitimar el gobierno comunista. El esfuerzo masivo iniciado por el gobierno de crear una presencia espacial dominante equivale a los gastos de los estados de crear enormes obras públicas que eran tan importantes para regímenes anteriores (y los modernos también, por ejemplo el sistema de carretera interestatal de la administración Eisen-

hower). Sin embargo, en un final, el propósito principal de una disputa de controlar, o al menos cerrar, el acceso al espacio tendría el mismo efecto general que la Gran Muralla original en mantener influencias extranjeras fuera del Reino Medio. Para China, el pasado siempre ha sido un prólogo.

Sin lugar a dudas, el énfasis en el espacio cada vez mayor de China y su antipatía cultural hacia la transparencia militar sugiere que un intento serio de controlar el espacio se está fraguando. Un temor persistente es la introducción repentina de una capacidad desconocida (llamémosle Tecnología X) que le permitiría a un estado hostil colocar rápida y económicamente armamento múltiple en la órbita. Las ventajas obtenidas de controlar el terreno elevado del espacio se acumularían al igual que a cualquier otro estado, mientras que la pérdida concomitante de poder militar de la negación del espacio a las fuerzas militares ya dependientes de Estados Unidos podría marcar el inicio de un reordenamiento del sistema internacional. Mientras más tiempo Estados Unidos vacile en sus responsabilidades militares, más probable un opositor posible pudiese apoderarse de la órbita baja de la Tierra antes que Estados Unidos pueda responder.

Y en esas circunstancias, Estados Unidos con certeza respondería. En cambio, si Estados Unidos armase el espacio, no es muy seguro del todo que cualquier otro estado o grupo de estados hallaría razonable contrarrestar del mismo modo. El costo inicial para proveer la infraestructura necesaria es aún demasiado elevado—como mínimo, cientos de billones de dólares. Los años de inversión que se necesitan para lograr una capacidad para lograr una contrafuerza comparable—esencialmente desde el inicio—le ofrecería más tiempo a Estados Unidos para atrincherarse en el espacio y contrarrestar esfuerzos preliminares para desplazarlo. El esfuerzo tremendo en tiempo y recursos sería peor que el desperdicio. La mayoría de los estados, si no todos, optaría por no contrarrestar *directamente* los despliegues de Estados Unidos. Puede que se opongan a los intereses estadounidenses con balance asimétrico, dependiendo de cuán agresivamente utilizan su nuevo poder, pero las probabilidades de una carrera armamentista hemorrágica en el espacio si Estados Unidos es el primero en desplegar armas—al menos durante los próximos años—son remotas.

Este razonamiento no disputa el hecho de que el despliegue de armas en el espacio exterior por parte de EE.UU. representaría la adición de una nueva capacidad militar potente, una que ayudaría a extender el periodo actual de hegemonía estadounidense hasta bien entrado el futuro. Obviamente esto sería amenazador, y Estados Unidos debe esperar condenas severas y mayor competencia en las áreas secundarias. Pero ese resultado es menos amenazador que otro estado, particularmente autoritario no liberal, lo haga. A pesar de que hay oposición obvia al balance de poder internacional actual, la mayoría de los estados parecen considerarlo como al menos tolerable. Una continuación del *status quo* es por lo tanto aceptable, como mínimo, inclusive para estados que están trabajando por su desaparición. Mientras que Estados Unidos no emplee su poder arbitrariamente, la situación se tomaría en cuenta al principio y se aceptaría a regañadientes con el transcurso del tiempo.

Aquí no aplica la imagen espejo. Un intento por parte de China de dominar el espacio sería parte de un intento de romper el dominio mar-aire de Estados Unidos en preparación para un nuevo orden internacional, con el estado que arme el espacio encima. Ese tipo de acción retaría el *status quo* en lugar de perpetuarlo. Esto sería desconcertante para las naciones que acepten el orden internacional actual—inclusive las instituciones venerables de comercio, finanza y leyes que operan dentro de él. Simultáneamente, sería intolerable para Estados Unidos. Como líder del sistema actual, Estados Unidos no podría hacer menos que participar en una carrera armamentista espacial ruinosa, salvo que se haga a un lado con elegancia y acepte un estatus mundial reducido.¹⁹

Apoderarse de la iniciativa y asegurar la órbita baja de la Tierra ahora, mientras que Estados Unidos domina en la infraestructura espacial, haría mucho por estabilizar el sistema internacional y evitaría una carrera armamentista en el espacio. La capacidad elevada de negarle a otra

nación cualquier intento de colocar recursos militares en el espacio y atacar rápidamente y destruir la capacidad anti satélite terrestre haría que la posibilidad de una guerra espacial a gran escala o carreras espaciales militares fuese *menos* probable, no más. Siempre que el estado que controla demuestre una capacidad y una voluntad de usar la fuerza para defender su posición, de hecho gastando una pequeña cantidad de violencia necesaria para evitar una mayor conflagración en el futuro, la probabilidad de una guerra futura *en* el espacio es remota.

Además, si Estados Unidos estuviese dispuesto a desplegar y emplear una fuerza espacial militar que mantuviese el control eficaz del espacio, y lo hiciese de manera que fuese percibida como fuerte, no arbitraria y eficaz, una acción de ese tipo serviría para desanimar a los estados en competencia de poner en servicio sistemas opuestos. También podría preparar el terreno para un régimen espacial nuevo, uno que fomentase el comercio y el desarrollo espacial. Si Estados Unidos utilizase su ventaja para vigilar los cielos y permitiera el uso pacífico y sin obstáculos del espacio por parte de cualquiera y todas las naciones para desarrollos económicos y científicos, con el tiempo su control de la órbita baja de la Tierra podría considerarse como un recurso global y un bien público. De la misma manera, los británicos mantuvieron el control de los mares en el siglo XIX, poniendo en vigor normas internacionales contra la esclavitud, el transporte de inocentes y derechos de propiedad, Estados Unidos podría preparar el espacio exterior para un brote de expansión económica que hace mucho tiempo se necesita.

Hay una sustentación histórica razonable para la noción que los periodos más pacíficos y prósperos en la historia moderna coinciden con un hegemon fuerte y liberal.²⁰ Durante los últimos sesenta años, Estados Unidos ha sido esencialmente incontestado es un su dominio naval y en la supremacía aérea global por los últimos quince años o más. Hoy, hay más comercio internacional en los océanos y en el aire que nunca. Buques y aeronaves de todas las naciones se preocupan más por tropezarse con mal tiempo que ser tomados a la fuerza por un buque militar o piratas. La búsqueda y rescate es una tarea mucho más común para la Armada que el embargo forzado y la transferencia de ayuda humanitaria es una misión regular. El legado del dominio militar estadounidense del mar y del aire ha sido positivo, y lo mismo se debe esperar para el espacio.

Conclusión

La geopolítica está en ascenso porque provee anteproyectos para la acción para aquellos que perciben el mundo en términos realistas. Halford Mackinder confirmó el principio primordial de la geoestrategia. Para dominar el espacio de batalla es necesario controlar las posiciones más vitales. Si éstas no se pueden controlar, entonces se deben disputar. El opositor no puede tener acceso sin inhibiciones. Este dictamen sencillo, conocido por cada estrategia y especialista en táctica, pero expresado tan claramente por Mackinder, es la esencia de la lógica del geoestratega. El control es deseable, pero la disputa es imperativa. Este dictamen aplica a cada medio y teatro de guerra.

Sin duda, Estados Unidos *mantendrá* la capacidad de influenciar las decisiones y los eventos más allá de sus fronteras, con la fuerza militar si fuese necesario. Si esta capacidad proviene del espacio al igual que de otros ámbitos militares no se ha determinado. Pero el despliegue operacional del armamento espacial aumentaría esa capacidad proporcionado proyección de fuerza mundial casi instantánea. Esa fuerza sería precisa, incontenible y letal. Estados Unidos mantendrá su posición de hegemonía al igual que su seguridad y el mundo no será amenazado por el espectro de un imperio estadounidense futuro. ▣

Notas:

1. Robert Strassler (ed), *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, traducido por Richard Crawley (New York: Free Press, 1996), p. 16.

2. Consultar Robert Gilpin, *War and Change in World Politics* (La guerra y el cambio en la política mundial) Cambridge: Cambridge University Press, 1981), para un recuento complete.
3. Para este análisis, recurro a definiciones por Geoffrey Parker, *Western Geopolitical Thought in the Twentieth Century* (Reflexión geopolítica occidental en el siglo XXI) (New York: St Martin's, 1986).
4. Strassler, *Thucydides* (Tucídides), pág. 352.
5. La postura del fundador del neorealismo, Kenneth Waltz, *Theory of International Relations* (Teoría de las relaciones internacionales) (New York: McGraw-Hill, 1979).
6. Jack Donnelly, *Realism and International Relations* (El realismo y las relaciones internacionales) (Cambridge: Cambridge University Press, 2000), págs. 43-4.
7. Alfred Thayer Mahan, *The Influence of Seapower Upon History: 1660-1783* (La influencia del poder marítimo en la historia: 1660-1783) (Boston: Little-Brown, 1890).
8. Halford Mackinder, *Democratic Ideals and Reality: A Study in the Politics of Reconstruction* (Los ideales democráticos y la realidad: Estudio en la política de la reconstrucción) (New York, Henry Holt, 1919).
9. Estas hipótesis se extrajeron de Everett Dolman, *Astropolitik: Classical Geopolitics in the Space Age I* (Astropolítica: Geopolítica clásica en la era espacial) (London: Frank Cass, 2002).
10. En términos de longevidad, menos como mínimo. Estas incluyen teorías económicas de interdependencia, funcionalismo y neo funcionalismo que conducen a la cooperación, y variantes de la supuesta teoría de paz democrática incluyendo la teoría de paz y de paz capitalista de Kant.
11. Sobre el dilema de la seguridad consultar a Robert Jervis, "Cooperation under the Security Dilemma" (La cooperación bajo el dilema de la seguridad) *World Politics*, Vol. 30, No. 2 (enero 1978), págs. 167-74.
12. Este argumento se le debe en gran medida a Francois Jullien, *A Treatise of Efficacy: Between Western and Chinese Thinking* (Tratado sobre la eficacia: Entre el modo de pensar occidental y el chino). Traducido por Janet Lloyd (Honolulu: University of Hawaii Press, 2004).
13. MacArthur estaba defendiendo su conducta en Corea. Para una contra opinión y crítica, consultar Everett Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (Pura estrategia: Poder y principio en la era espacial y de la informática) (London: Frank Cass, 2004, págs. 6-7. Para un recuento positivo, consultar Theodore y Donna Kinni, *No Substitute for Victory: Lessons in Leadership from Douglas MacArthur* (No hay sustituto para la victoria: Lecciones de Douglas MacArthur sobre el liderazgo) (Upper Saddle River, NJ: FT Press, 2005).
14. Sun Tzu, *Art of War* (El arte de la guerra), traducido por Ralph Sawyer (Boulder, CO: Westview Press, 1994), pág. 177.
15. Esta sección se extrajo de una discusión mucho más completa sobre los papeles que desempeñan la estrategia, las operaciones y la táctica en Dolman, *Pure Strategy* (Pura estrategia).
16. Un argumento adaptado de una afirmación económica expresada por David Baldwin, *Economic Statecraft* (Política económica) (Princeton NJ: Princeton University Press, 1985), págs. 6-15.
17. John Hickman y Everett Dolman, "Resurrecting the Space Age: A State-Centered Commentary on the Outer Space Regime" (Resuscitando la era espacial: Un comentario centrado en el estado sobre el régimen del espacio exterior) *Comparative Strategy*, Volumen 21, Número 1 (2002), págs. 1-19).
18. Para una postura apologista, consultar Li Jiuquan, "Legality and Legitimacy: China's ASAT Test" (Legalidad y legitimidad: La prueba ASAT de China) *China Security*, Vol 5, Núm. 1, invierno 2009, págs. 43-52.
19. Después de la teoría de la estabilidad hegemónica (HST) según esbozada por Duncan Snidal, "The Limits of Hegemonic Stability Theory" (Los límites de la teoría de la estabilidad hegemónica), *International Organization*, Volumen 39: Núm. 4 (Otoño) 1985, págs. 579-613.
20. Immanuel Wallerstein, "The Rise and Future Demise of the World Capitalist System: Concepts for Comparative Analysis" (El origen y la desaparición futura del sistema capitalista mundial: Conceptos para una análisis comparativo) y *Comparative Studies in Society and History* (Estudios comparativos en la sociedad y en la historia, Vol. 16 (1974)), págs. 387-415.

El Dr. Everett Carl Dolman es profesor de estudios militares comparativos en la Escuela de Estudios Avanzados Aéreos y Espaciales de la USAF (SAASS), donde se le ha identificado como el primer teórico espacial de la Universidad del Aire. Entre sus obras publicadas se encuentran las siguientes: *Astropolitik: Classical Geopolitics in the Space Age* (Frank Cass, 2002); *The Warrior State: How Military Organization Structure Politics* (El estado guerrero: Cómo una organización militar estructura la política) (Palgrave, 2005); y *Pure Strategy: Power and Principle in the Space and Information Age* (Routledge, 2005). El Dr. Dolman es también cofundador y editor de *Astropolitics: The International Journal of Space Power and Policy*.

Justificación de un Comando Combatiente del Ciberespacio

Combinar las Responsabilidades y Autorizaciones del Servicio y el Comando Combatiente

TENIENTE CORONEL SHAWN M. DAWLEY, AIR NATIONAL GUARD

EL SIGUIENTE ANTEPROYECTO del *Plan de Comando Unificado* debería volver a designar al Comando del Ciberespacio de los Estados Unidos como un comando combatiente (COCOM) funcional. Así como muchos en el liderazgo del Ejército Estadounidense deseaban relegar al Cuerpo Aéreo del Ejército a simple apoyo de las operaciones de guerra terrestre, los militares actuales ejercitan de forma rutinaria capacidades del ciberespacio en apoyo de funciones que habilitan operaciones en otros dominios. Poner al Comando del Ciberespacio de los Estados Unidos (USCYBERCOM) en el mismo nivel que otros COCOM geográficos y funcionales, y otorgarles autoridad para organizar, adiestrar y equipar a sus fuerzas subordinadas le permitirá desarrollar, emplear y explotar capacidades dentro de este reciente campo de acciones de guerra.

Aunque creado por el hombre, el ciberespacio sigue siendo un dominio en el que los participantes pueden actuar y reaccionar, asemejándose de esta manera a los dominios aéreo, marítimo y terrestre. Como en los conflictos anteriores, haciendo historia, cualquier tribu, elemento criminal o nación estado que no transforme en armas adecuadamente sus capacidades en la lucha de guerra puede verse incapaz de librar combate con éxito en el espectro del conflicto armado. Debido a la naturaleza no cinética del ciberespacio, las batallas institucionales y doctrinarias sobre la organización y el empleo de las capacidades del ciberespacio de los Estados Unidos han tendido a centrarse en sus características habilitadoras en lugar de su capacidad ofensiva. Las normas organizativas, de adquisición y puesta en funcionamiento del Departamento de Defensa (DOD) colocan al poderío aéreo en el dominio aéreo, al poderío naval en el dominio marítimo, y al poderío terrestre en el dominio terrestre. Tal como lo enuncia el General Peter Pace, USMC, retirado, ex jefe del Estado Mayor Conjunto, “la integración de operaciones ofensivas y defensivas en el ciberespacio, junto con la destreza y conocimiento de nuestra gente, es fundamental” para asegurar superioridad estratégica en el dominio del ciberespacio.¹

Aunque los otros dominios de lucha de guerra existían mucho antes que la capacidad de la gente para operar dentro de ellos, existe un vínculo inexorable entre el dominio del ciberespacio y las capacidades dentro de este—así como las herramientas y doctrinas evolucionan, también lo hace el medio. Este componente evolucionario probablemente hará que el ciberespacio se convierta en el área más impredecible dentro del espectro total del conflicto. Adoptar esta realidad posiblemente requiere un enfoque y una estructura organizacional que no solo acepte sino anime la no conformidad y guerreros menos convencionales.

Una guerra cinética en gran escala generalmente premia a las fuerzas que son resueltamente disciplinadas y están basadas en doctrina sólida (dado el número de combatientes involucrados y la estrecha coordinación necesaria para ejecución). Sin embargo, una fuerza mucho más pequeña puede realizar ciberguerra, premiando la rapidez y agilidad en el ciberespacio en una magnitud mayor que en los espacios de batalla tradicionales. Así, si estas suposiciones son válidas, un esfuerzo en el ciberespacio puede requerir operadores menos inclinados a seguir fielmente la doctrina establecida y que una entidad los organice y emplee, a diferencia de las cons-

trucciones tradicionales del servicio o COCOM. El actual modelo organizacional dentro del *Plan de Comando Unificado* coloca al recientemente formado USCYBERCOM conjunto como un comando subunificado bajo el Comando Estratégico Estadounidense. Los militares necesitan un concepto que combine las autoridades del servicio y combate de guerra en un solo cuerpo y eleve a esa organización hasta un nivel en que pueda sacar máximo provecho del ciberespacio. Con esa finalidad, debe convertir al USCYBERCOM en un COCOM pleno y funcional y otorgarle al comando las autorizaciones de presupuesto bajo el título 10, *Código de los Estados Unidos*, para organizar, adiestrar y equipar a su contingente singular de guerreros.

Estrategia y ejecución

Aunque las costumbres duraderas, las normas internacionales, y los conflictos armados han instituido el reconocimiento casi universal de la soberanía física, la noción de las naciones-estado sobre el dominio físico es menos exigente en las discusiones sobre el dominio del ciberespacio. Desde la Paz de Westfalia a mediados del siglo diecisiete, la soberanía ha sido considerada como una autoridad legítima sobre las posesiones territoriales.² Así, por más de 300 años, los gobiernos, monarquías o repúblicas por igual, pudieron delinear físicamente usurpaciones sobre sus territorios por fuerzas de tierra, mar y—eventualmente aire. Más aún, la destrucción física de una fortaleza o institución financiera constituía indiscutiblemente un acto de guerra. En el dominio del ciberespacio, las acciones no cinéticas producen los mismos efectos, dejando al agraviado sin el mismo sentido de actividad hostil. Pero un ataque de red de computadoras que deje a un puesto de comando de una brigada de tiro incapaz de localizar blancos o un virus que “se centre” en las cuentas de un sistema bancario no es *completamente* diferente de bombas que arrasen a cualquiera de ellos. La distinción principal es que un ataque cinético proporciona un “efecto CNN” tangible mientras que uno que solo utiliza código binario carece de la pasión tan crítica para que se exijan represalias.

Como los ataques o exploraciones pueden suceder (y suceden) dentro del dominio del ciberespacio—pero no en la misma forma en que ocurren en los otros dominios—las naciones-estado deben actualizar la tradición doctrinal de la teoría de la guerra justa. Particularmente en relación al *derecho de guerra* (*jus ad bellum*), “que concierne a la justicia de recurrir a la guerra en primer lugar”, muchos estudiosos de asuntos internacionales sostienen que solo en las secuelas de una amenaza, existencial o de otro tipo, debe una nación-estado recurrir al conflicto.³ Hasta la fecha, tales amenazas se han dirigido generalmente contra posesiones físicas. La presencia de computadoras, torres de teléfonos celulares y redes de comunicaciones en la vanguardia en cualquier ciberguerra evita la defensa a profundidad.⁴ Fundamentalmente, como las vulnerabilidades del ciberespacio incluyen su dependencia en sistemas de redes interconectados no patentados que operan los civiles, “no disponemos de un sistema de radar de alerta temprana ni de Guardia Costera que patrulle las fronteras en el ciberespacio”.⁵ Por lo tanto, consistente con la doctrina Bush, que considera la guerra preventiva como el contrarresto necesario a las amenazas asimétricas planteadas por actores hostiles que utilizan armas de destrucción masiva, un enfoque acertado para el ciberespacio une la postura defensiva con las capacidades ofensivas, preventivas.

Operaciones en el ciberespacio y guía estratégica

Gran parte de la atención dada al ciberespacio y la ciberguerra (guerra en el ciberespacio) en el planeamiento estratégico trata de las amenazas contra Estados Unidos y sus aliados en lugar de la necesidad de armar la cibercapacidad amigable. En la *Estrategia de Seguridad Nacional*, *Estrategia de Defensa Nacional*, y *Estrategia Militar Nacional de los Estados Unidos de América* más recientes, los líderes superiores del gobierno y militares enfatizan los peligros que plantean los actores es-

tado y no estado que tienen capacidad de realizar ciberataques contra Estados Unidos y sus aliados. Ponen menos atención en el desarrollo de una robusta capacidad de “lanzar ataques”. Naturalmente, como estas publicaciones tienen una audiencia nacional e internacional, no se esperaría que contengan datos específicos sobre las capacidades ofensivas. Al mismo tiempo, el grado al cual estos documentos exploran las vulnerabilidades de nuestra nación en el dominio del ciberespacio excede de lejos la atención prestada a generar poder de combate.

En la *Estrategia de Seguridad Nacional* (2010), el Presidente Barack Obama reconoce la importancia de la ciberseguridad, considerándola como uno de los seis imperativos estratégicos para salvaguardar los intereses nacionales estadounidenses: “Además de enfrentar enemigos en los campos de batalla tradicionales, Estados Unidos debe estar preparado para las amenazas asimétricas, como aquellas que amenazan nuestra dependencia en el espacio y el ciberespacio”.⁶ Este y otros pasajes preparados por su personal de seguridad nacional y presentado en ese documento tratan en su mayor parte con las vulnerabilidades estadounidenses. La estrategia captura y proyecta con precisión la naturaleza de las ciberamenazas futuras como existentes a través del continuo de adversarios potenciales. Sin embargo, presenta el rol facilitador del ciberespacio exclusivo de su capacidad ofensiva: “Las amenazas que enfrentamos varían desde hackers criminales individuales hasta . . . redes terroristas y naciones-estado avanzadas. . . . Por lo tanto, nuestra infraestructura digital, es un activo nacional estratégico. . . . Disuadiremos, impediremos, detectaremos y nos defenderemos contra los ataques e intrusiones ciberespaciales y nos recuperaremos rápidamente de ellos”.⁷

Al igual que la *Estrategia de Seguridad Nacional*, la *Estrategia de Defensa Nacional* (2008) reconoce que la susceptibilidad del ciberespacio a las operaciones maliciosas es una vulnerabilidad estratégica. Más aún, también carece de pautas sólidas y significativas sobre la forma de avanzar la ingeniería ofensiva de las capacidades del ciberespacio: “Estados Unidos . . . y nuestros socios enfrentan un espectro de *desafíos*, incluyendo . . . el espacio emergente y las ciberamenazas” (énfasis añadido).⁸ Los peligros del ciberespacio están agrupados correctamente con el grupo de amenazas no convencionales potenciales, pero la *Estrategia de Defensa Nacional* los presenta únicamente como un *desafío*—no como una oportunidad para explotación. Además, la estrategia tiende a ser más rígida que la guía estratégica del presidente en cuanto a que asocia más fácilmente las ciberamenazas con la guerra asimétrica contra Estados Unidos por un adversario más débil: “Grupos pequeños o individuos . . . pueden atacar puntos vulnerables en el ciberespacio . . . causando daño económico, comprometiendo información y materiales sensibles, e interrumpiendo servicios críticos como redes de electricidad y de información”.⁹

Finalmente, la *Estrategia Militar Nacional de los Estados Unidos de América* (2011) considera al ciberespacio no simplemente como un “talón de Aquiles” potencial sino como un dominio en el que Estados Unidos puede y debe *ejecutar* operaciones. Acepta abiertamente los desafíos inminentes a la capacidad habilitadora del ciberespacio cuando estipula que “el acceso asegurado y la libertad de maniobra dentro de los bienes globales comunes—áreas compartidas de mar, aire y espacio—y los dominios globalmente conectados como el ciberespacio están siendo desafiados con más frecuencia por actores estado y no estado”.¹⁰ Sin embargo, la estrategia se aparta de sus documentos antecesores emitidos por el presidente y el secretario de defensa cuando establece que “la habilitación y los dominios de *lucha de guerra* del espacio y el ciberespacio son más críticos para nuestras operaciones, aunque más vulnerables a las acciones maliciosas” (énfasis añadido).¹¹ Aquí, un lector de orientación política estratégica obtiene una primera mención del ciberespacio como un medio en el que tiene lugar la guerra, aunque principalmente no cinética. Este contexto de doble propósito es comparable al de cualquier otro dominio. Por ejemplo, en el dominio aéreo, se puede realizar reabastecimiento aéreo de bases de operaciones de avanzada (una función habilitadora) o bombardeos de columnas blindadas (una función de lucha de guerra). Más concretamente, la *Estrategia Militar Nacional* declara que “el espacio y el ciberespa-

cio habilitan la lucha de guerra global efectiva en los dominios aéreo, terrestre y marítimo, y *han surgido como dominios de lucha de guerra por propio derecho*” (énfasis añadido).¹²

Además del documento de estrategia del Presidente del Estado Mayor Conjunto, el panorama en el *Entorno Operativo Conjunto* hace evaluaciones comparables sobre la dinámica cambiante del ciberespacio. Aborda amenazas *dentro* del ciberespacio, como su conversión en un “frente principal en conflictos irregulares y tradicionales”, y también la gama de *adversarios* desde “estados y no estados . . . desde el hacker aficionado no sofisticado hasta los hackers profesionales altamente capacitados”.¹³ Sin embargo, encontramos un pedido más directo a la acción, en la *Lista Universal de Tareas Conjuntas* (bajo “Administración de Operaciones del Ciberespacio”), que encarga a los “servicios y agencias el asegurar que las capacidades *ofensivas* y defensivas estén desplegadas y listas para reforzar los objetivos de seguridad nacional . . . del DOD y de los Estados Unidos en el ciberespacio (énfasis añadido).¹⁴ Aunque carece de la exigencia de la *Lista de Tareas Conjuntas* de una capacidad ofensiva dentro del ciberespacio, el *Entorno Operativo Conjunto* plantea un desafío—como también lo hace la *Estrategia Militar Nacional*—para reconsiderar el concepto organizacional y doctrinario de los esfuerzos del DOD en el ciberespacio.

En el *Entorno Operativo Conjunto*, se puede leer que “aunque se ha avanzado hacia la definición de requisitos y en propugnar por fuerzas ciberespaciales del Servicio, las ciberamenazas demandarán una nueva mentalidad para garantizar agilidad de adaptación a los nuevos desafíos”.¹⁵ Igualmente, pero con más énfasis en los asuntos organizacionales del futuro, la *Estrategia Militar Nacional* plantea que “revisaremos cuidadosamente los sistemas de personal existentes. . . . El dominio de lucha de guerra en el ciberespacio requiere especial atención en este aspecto”.¹⁶ Dentro de los parámetros de estos vectores estratégicos de “nueva mentalidad”, “agilidad” y personal, hay campo para enfocar las capacidades, funciones y misiones del ciberespacio *no* como extrapolaciones de organizaciones y doctrinas existentes sino como problemas únicos dignos de soluciones innovadoras.

En los niveles de COCOM y del servicio, los enfoques de abajo-arriba con respecto a la ciber guerra se han dividido más apropiadamente entre mantener el acceso a las funciones habilitadoras del ciberespacio (defensivas) y la capacidad de explotar y atacar las redes del adversario (ofensivas):

USCYBERCOM es responsable de planificar, coordinar, integrar, sincronizar, y dirigir actividades para operar y defender las redes de información del Departamento de Defensa y, cuando se le ordene, realizar operaciones militares de espectro total en el ciberespacio. . . con el fin de garantizar la libertad de acción estadounidense y aliada en el ciberespacio, *mientras que a la vez niega lo mismo a nuestros adversarios*.¹⁷ (énfasis añadido)

La frase “negar lo mismo” expresa una aplicación deliberada y activa de la capacidad del ciberespacio contra un enemigo para crear efectos de manera consistente con operaciones basadas en efectos, que se “planeen, ejecuten, evalúen, y adapten para influenciar o cambiar los sistemas o capacidades con el fin de lograr resultados deseados.”¹⁸ Vinculando acciones a objetivos, se pueden generar efectos de forma cinética o no cinética. La utilización de capacidades del ciberespacio para afectar nodos dentro de un sistema—especialmente dentro de un sistema de sistemas—puede crear efectos cuyos resultados exceden enormemente las entradas. Como la guerra es compleja y no lineal, una pequeña ciberacción contra una construcción nodal puede producir consecuencias perturbadoras.

Un modelo de comando combatiente

Según la Publicación Conjunta No. 1, *Doctrina de las Fuerzas Armadas de los Estados Unidos*, los COCOM funcionales son “responsables de un área funcional grande que requieren responsabilidad única para la coordinación efectiva de las operaciones de dicho plan. Estas responsabilidades son normalmente globales por naturaleza”.¹⁹ Más allá de esta orientación operativa, el Co-

mando de Operaciones Especiales de los Estados Unidos (USSOCOM) también combina autoridades y responsabilidades *similares a las del servicio* con aquellas típicamente asociadas con otros COCOM funcionales. Como un híbrido de un servicio y un COCOM (por ejemplo, la Marina Estadounidense y el Comando Central Estadounidense), el USSOCOM prepara fuerzas para desplegarlas y luego desempeña una función cuando entran en batalla.

Después de la aprobación de la Ley de Reorganización de la Defensa de 1986, se estableció el USSOCOM como un comando unificado de cuatro estrellas “responsable de preparar Fuerzas de Operaciones Especiales para realizar misiones asignadas y, si lo ordena el Presidente o el Secretario de Defensa, planear y llevar a cabo operaciones especiales”.²⁰ El primer encargo, “preparar Fuerzas de Operaciones Especiales”, es comparable al de cualquier servicio; el segundo, “planear y llevar a cabo operaciones especiales”, cae dentro del área normalmente asociada con un COCOM.

El *Plan de Comando Unificado* de 2004 “asignó al USSOCOM la responsabilidad de sincronizar planes del Departamento de Defensa contra redes terroristas globales y, cuando se le ordene, realizar operaciones globales [contra esas redes]”.²¹ Para hacerlo, el comando “recibe, revisa, coordina y prioriza los planes del DoD . . . y hace recomendaciones al Estado Mayor Conjunto en relación a asignaciones de fuerzas y recursos para cumplir requisitos globales”.²²

Si USSOCOM cumple obligaciones parecidas a las del servicio para desarrollar una fuerza y autoridades parecidas a las del COCOM para emplearla, entonces el comando mantiene una organización que

1. desarrolla estrategia y doctrina para enfrentar desafíos únicos;
2. tiene autoridad presupuestal para reclutar, organizar, adiestrar y equipar personal seleccionado;
3. puede proveer recursos a los COCOM en una función de apoyo; y
4. puede conducir operaciones a nivel mundial en una función apoyada.

Esta combinación de responsabilidades título 10 al estilo del servicio con autoridades al estilo del COCOM establece una organización con un mandato mundial que puede asignar el personal correcto a la misión; desarrollar tácticas, técnicas y procedimientos ágiles; y librar guerras contra el enemigo en todo el espectro del conflicto. USCYBERCOM debería adoptar este modelo.

Recomendaciones

Un COCOM funcional que reclute, organice, adiestre, equipe y emplee capacidades del ciberespacio como armas en el más nuevo dominio de la guerra es esencial para el conflicto contemporáneo. Así como el Comando de Operaciones Especiales de la Fuerza Aérea, el Comando de Operaciones Especiales de la Infantería de Marina, el Comando de Operaciones Especiales del Ejército, y el Comando de Guerra Especial de la Marina son comandos componentes del USSOCOM, el Cibercomando de Fuerzas del Ejército, la Vigésimo Cuarta Fuerza Aérea, el Cibercomando de Flota, y el Cibercomando de Fuerzas de la Infantería de Marina retendrían sus afiliaciones como componentes de servicio del USCYBERCOM.²³ Al igual que los componentes que actualmente forman el USSOCOM, los componentes del USCYBERCOM aumentado deberán incluir personal único y adecuado para su misión central.

Los actuales modelos de personal demuestran la efectividad de una proporción grande de “personal de apoyo por cada soldado en combate (tooth-to-tail)” para ciertas construcciones de fuerza. De los casi 60.000 miembros de USSOCOM, sólo unos 20.000 son “operadores”—individuos reclutados, adiestrados y retenidos como fuerzas especiales.²⁴ Analizando otra comunidad por contexto, la de aeronaves a control remoto, vemos que el número de pilotos y operadores de

sensores representa solo una fracción del personal total requerido. Este modelo refuerza el concepto de un centro de operaciones en el ciberespacio controlado centralmente, ya que los operadores de misión de estas aeronaves pueden realizar funciones globales desde una guarnición separada geográficamente.

La proporción de personal de apoyo a operadores del ciberespacio necesita más investigación, pero es más probable que los operadores reciban apoyo de un mayor número de especialistas administrativos y técnicos. De manera similar a las “Verdades de las SOF [fuerzas de operaciones especiales]” del Ejército estadounidense que “calidad es mejor que cantidad” y que “los humanos son más importantes que el equipo”, no todo “soldado del ciberespacio” tiene que ser un cazador matador.²⁵ Más bien, la mayor parte de USCYBERCOM incluiría al personal administrativo y de apoyo logístico que conforma cualquier otro comando, con énfasis en reclutar, adiestrar, equipar y retener deliberadamente a aquellos hombres y mujeres seleccionados más idóneos para las misiones duales de ciber-defensa y ciber-ataque.

A continuación de, o junto con, una revisión del *Plan de Comando Unificado*, la acción legislativa proporcionaría autoridad presupuestal a USCYBERCOM—como la de los servicios y USSOCOM—y especificaría funciones y misiones. Esto hace necesario un cambio en el título 10 *Código de los Estados Unidos* (Fuerzas Armadas), Parte 1 (Organización y Poderes Militares Generales), Capítulo 6 (Comandos Combatientes). Aparte de concebir normas para incorporar el cambio estatutario antes mencionado en el estado del USCYBERCOM, el DOD necesitaría revisar su proceso de planeamiento, programación, presupuesto y ejecución.²⁶ Tal como el Programa de Fuerza Principal 11, Operaciones Especiales (MFP-11) en el *Programa de Defensa para Años Futuros*, el DOD deberá establecer un programa de fuerza principal dedicado (por ejemplo, “MFP-12 Ciberoperaciones”), junto con una entrada presupuestal para USCYBERCOM (similar a la que actualmente tienen USSOCOM, los servicios y las agencias del DOD).²⁷

Finalmente, para librar guerra en el ciberespacio, se deberá establecer una fuerza de cibertareas conjunta (JCTF) con USCYBERCOM. Actuando como celda de fusión para monitoreo mundial de ciberamenazas y como autoridad de comando a través de la cual el secretario de defensa, en comunicación con el Estado Mayor Conjunto, puede ordenar al USCYBERCOM que lleve a cabo su misión de COCOM, esta JCTF planearía y dirigiría operaciones ofensivas y de contraataque dentro del ciberespacio contra el espectro de adversarios que amenazan los intereses nacionales estadounidenses, el ciberespacio o de otra clase.

Conclusión

Un USCYBERCOM con la autorización para organizar, adiestrar, y equipar sus fuerzas y emplearlas contra los adversarios puede desarrollar y explotar mejor las capacidades dentro del más nuevo dominio de la guerra. Mientras una ciberfuerza permanezca subordinada a la potencial mentalidad pueblerina del servicio o de lucha de guerra tradicional, será difícil transformar en armas su capacidad para infligir efectos en el espacio de batalla. Si se proporciona a los líderes más libertad de movimiento dentro de la burocracia del DOD, USCYBERCOM les permitirá desarrollar y mantener poder de combate en una forma menos obstaculizada por los enfoques convencionales de sus respectivas ramas—como fue el caso de someter a reevaluación al poderío aéreo como una capacidad que superó sus efectos de apoyo a la doctrina del campo de batalla del Ejército. Una vez que sus fuerzas estén totalmente desarrolladas y disponibles, un USCYBERCOM con autoridad de COCOM funcional para realizar operaciones contra sistemas nodales estará posicionado para crear efectos desproporcionados y potencialmente catastróficos. Estos efectos—algunos de los cuales se pueden “deshacer”, dada su naturaleza a menudo no cinética—pueden producirse mediante aplicación precisa de un JCTF permanente. □

Notas

1. Presidente del Estado Mayor Conjunto, *The National Military Strategy for Cyberspace Operations (La Estrategia Militar Nacional para Operaciones en el Ciberespacio)* (Washington, DC: Presidente del Estado Mayor Conjunto, diciembre de 2006), vii, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

2. Eleonore Kofman y Gillian Youngs, editores, *Globalization: Theory and Practice (Globalización: Teoría y Práctica)* (New York: Pinter, 1996), 111.

3. *Stanford Encyclopedia of Philosophy (Enciclopedia Stanford de Filosofía)*, edición otoño de 2008, s.v. “War,” <http://plato.stanford.edu/archives/fall2008/entries/war/>.

4. Comando de Fuerzas Conjuntas de los Estados Unidos, *The Joint Operating Environment (El entorno operativo conjunto)* (Suffolk, VA: Comando de Fuerzas Conjuntas de los Estados Unidos, Grupo de Operaciones Futuras Conjuntas, 18 de febrero de 2010), 34–36, http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf.

5. Forrest Hare, “Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? (Fronteras en el ciberespacio: ¿Puede la soberanía adaptarse a los desafíos de la ciberseguridad?)”, en *The Virtual Battlefield: Perspectives on Cyber Warfare (Campo de batalla virtual: Perspectivas sobre la guerra en el ciberespacio)*, editores Christian Czosseck y Kenneth Geers, Cryptology and Information Security Series, vol. 3 (Fairfax, VA: Ios Press, 2009), 5.

6. Presidente de los Estados Unidos, *National Security Strategy (Estrategia de Seguridad Nacional)* (Washington, DC: la Casa Blanca, mayo de 2010), 17, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

7. *Ibid.*, 27.

8. Departamento de Defensa, *National Defense Strategy (Estrategia de Defensa Nacional)* (Washington, DC: Departamento de Defensa, junio de 2008), 1, <http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf>.

9. *Ibid.*, 7.

10. Estado Mayor Conjunto, *National Military Strategy of the United States of America (Estrategia Militar Nacional de los Estados Unidos de América)* (Washington, DC: Estado Mayor Conjunto, 2011), 3, http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.

11. *Ibid.*

12. *Ibid.*, 9.

13. Comando de Fuerzas Conjuntas de los Estados Unidos, *Joint Operating Environment (Entorno Operativo Conjunto)*, 36.

14. *Universal Joint Task List (Lista Universal de Tareas Conjuntas)*, versión 7.1, 17 de julio de 2012, [244], http://www.dtic.mil/doctrine/training/ujtl_tasks.pdf.

15. Comando de Fuerzas Conjuntas de los Estados Unidos, *Joint Operating Environment (Entorno Operativo Conjunto)*, 36.

16. Estado Mayor Conjunto, *National Military Strategy (Estrategia Militar Nacional)*, 17.

17. “U.S. Cyber Command (Comando del Ciberespacio de los Estados Unidos)”, Comando Estratégico de los Estados Unidos, diciembre de 2011, http://www.stratcom.mil/factsheets/Cyber_Command/.

18. Documento de Doctrina de la Fuerza Aérea 2, *Operations and Organization (Operaciones y Organización)*, 3 de abril de 2007, 13, <http://www.e-publishing.af.mil/shared/media/epubs/afdd2.pdf>.

19. Publicación conjunta 1, *Doctrine for the Armed Forces of the United States (Doctrina de las Fuerzas Armadas de los Estados Unidos)*, 2 de mayo de 2007 (Incorpora el cambio 1, 20 de marzo de 2009), I-14, http://www.dtic.mil/doctrine/new_pubs/jpl1.pdf.

20. “Comando de Operaciones Especiales (SOCOM) de los Estados Unidos”, Departamento de Defensa de los Estados Unidos, consultado el 9 de noviembre de 2012, <http://www.defense.gov/OrgChart/office.aspx?id=62>.

21. “About USSOCOM (Sobre el USSOCOM)”, Comando de Operaciones Especiales de los Estados Unidos, consultado el 9 de noviembre de 2012, <http://www.socom.mil/Pages/AboutUSSOCOM.aspx>.

22. *Ibid.*

23. “U.S. Cyber Command Fact Sheet (Ficha de datos del Comando del Ciberespacio de los Estados Unidos)”, Departamento de Defensa de los Estados Unidos, 25 de mayo de 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.

24. Senado, *Audiencias ante la Comisión sobre Servicios Armados para autorizar las asignaciones del año fiscal 2012 para las actividades militares del Departamento de Defensa y para construcciones militares, para prescribir los números de personal militar para el año fiscal 2012, y para otros fines*, Congreso No 112, primera sesión, <http://www.gpo.gov/fdsys/pkg/CHRG-112shrg68084/html/CHRG-112shrg68084.htm>. En este documento, véase Comando de Operaciones Especiales de los Estados Unidos y Comando Central de los Estados Unidos, 1 de marzo de 2011, y la declaración de postura del Almirante Eric T. Olson, USN, comandante, Comando de Operaciones Especiales de los Estados Unidos.

25. “SOF Truths (Verdades de las SOF)”, Comando de Operaciones Especiales de los Estados Unidos, consultado el 9 de noviembre de 2012, <http://www.soc.mil/USASOC%20Headquarters/SOF%20Truths.html>.

26. "Planning, Programming, Budgeting & Execution Process (PPBE) (Biennial Driven) [Proceso de planificación, programación, presupuesto y ejecución (realizado cada dos años)]," Defense Acquisition University, 27 de septiembre de 2012, <https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=10fdf6c0-30ca-43ee-81a8-717156088826>.

27. Departamento de Defensa, *Future Years Defense Program (FYDP) Structure [Estructura del Programa de Defensa para Años Futuros (FYDP)]* (Washington, DC: Departamento de Defensa, Oficina del Director, Análisis y Evaluación de Programas, abril de 2004), 6, <http://www.dtic.mil/whs/directives/corres/pdf/704507h.pdf>; y Mayor Robert Siau, comandante, Destacamento del Escuadrón del Comunicaciones de Combate No 143, Washington Air National Guard, conversación con el autor, marzo de 2011.



El Teniente Coronel Shawn M. Dawley, ANG (BS, MBA, Embry-Riddle Aeronautical University; MA, Marine Corps University; MA, American Military University) es comandante del 165º Escuadrón de Transporte Aéreo, Guardia Nacional Aérea de Kentucky. Es piloto de aviones C-130 y ha volado misiones de combate y de apoyo de combate en apoyo a la Operación Libertad Duradera, Operación Libertad para Irak, Operaciones Joint Forge y Joint Guard y la Operación Southern Watch. Recientemente se desempeñó en calidad de comandante del 737º Escuadrón Expedicionario de Transporte Aéreo en el Sudoeste de Asia. El Tte Cnel Dawley completó la Escuela Superior para Oficiales de Escuadrón, la Escuela Superior de Comando y Estado Mayor de la Fuerza Aérea, la Escuela Superior de Comando y Estado Mayor del Cuerpo de Infantería de Marina, la Escuela Superior de Guerra de la Fuerza Aérea y la educación militar profesional conjunta avanzada de la Escuela Superior de Estado Mayor de la Fuerza Conjunta.

Sin Lugar Para Esconderse

La Creciente Amenaza Para Las Bases Aéreas

CORONEL SHANNON W. CAUDILL, USAF

MAYOR BENJAMÍN R. JACOBSON, USAF

VISTIENDO UNIFORMES del ejército estadounidense, los atacantes atravesaron las defensas de la base aérea ocultos por la oscuridad de la noche. Armados de rifles, lanzagranadas propulsadas por cohete, y chalecos suicidas, el grupo de 14 hombres inició su misión mortal contra una base aérea en la Provincia de Helmand, Afganistán, una base con personal de la Fuerza Internacional de Asistencia de Seguridad (ISAF) de la Organización del Tratado del Atlántico Norte (OTAN). El combate duró varias horas, y el amanecer reveló la destrucción de seis aviones a reacción AV-8B Harrier y daños a otras dos aeronaves; además, “sufrieron daños seis hangares”, y “quedaron destruidas seis estaciones de reabastecimiento de combustible”.¹ En el ataque, murieron 14 insurgentes y dos infantes de marina estadounidenses mientras que ocho miembros militares y un contratista de la coalición fueron heridos. En septiembre de 2012, esta operación insurgente constituyó el ataque terrestre más exitoso hasta la fecha contra activos aéreos de la ISAF de la OTAN en el conflicto de Afganistán.

El General italiano Giulio Douhet dijo una vez que “es más fácil y más efectivo destruir el poderío aéreo del enemigo atacando sus nidos y huevos en el suelo que cazar sus aves voladoras en el aire”.² La observación de Douhet es aún válida, como se demostró con el ataque antes mencionado contra la base aérea Helmand. De hecho, las bases aéreas deficientemente defendidas seguirán siendo susceptibles a los asaltos por tierra. Con anterioridad, a arremetida más exitosa contra una base aérea después de la guerra de Vietnam había ocurrido durante la guerra civil en El Salvador en 1982, donde unos 100 rebeldes atacaron una base de la Fuerza Aérea Salvadoreña, destruyendo cinco aeronaves Ouragan, seis UH-1B y tres C-47 a la vez que dañaron otras cinco plataformas. Evidentemente, esta “operación bien planeada y ejecutada . . . demostró la superioridad táctica” de los insurgentes contra la fuerza gubernamental de defensa de la base.³

En el futuro, la complejidad y el costo de proteger bases aéreas y los activos del aire y el espacio crecerán exponencialmente debido a las nuevas tecnologías, la abundancia de información de dominio público, y el desarrollo de la capacidad del adversario. Las amenazas tradicionales como asaltos aerotransportados, fuego indirecto (IDF) mediante cohetes y morteros, y ataques directos con escuadrones suicidas continuarán siendo las opciones básicas de la acción enemiga. En consecuencia, debemos examinar las amenazas emergentes que hacen posible nuevos modos de ataque a bases aéreas, incluyendo el desarrollo de municiones de precisión, la propagación de vehículos a control remoto (RPV), la proliferación de misiles superficie-aire (SAM) disparados desde el hombro que son una creciente la amenaza interna, y otras variantes de una nueva bonanza tecnológica para terroristas e insurgentes. La defensa de los activos aéreos se volverá aún más problemática frente a un espectro de amenazas habilitadas por la tecnología y una aceleración de la amenaza interna. Este desarrollo y proliferación de tecnologías permitirá que los grupos pequeños logren una ventaja aún mayor contra los defensores de bases y operadores aéreos.

Evidentemente, los Aerotécnicos deben considerar seriamente la alta probabilidad de estas amenazas emergentes y los costos asociados de garantizar las operaciones continuas. Anteriormente, un hombre y un rifle cubrían una brecha en un sector de defensa de la base. Las bases aéreas bien defendidas obligan al enemigo a explorar medios alternativos de afectar las operaciones aéreas. Naturalmente, cualquier actor racional quiere lograr el camino al éxito más rá-

pido y de menor costo después de seleccionar el objetivo. Si no está buscando un ataque espectacular diseñado para producir bajas e imágenes dramáticas de televisión (como fomentan los grupos tipo al-Qaeda), posiblemente deseará impedir la continuidad de las operaciones aéreas y desgastar a la base mediante un acoso que produzca víctimas en transcurso del tiempo.

Sin embargo, al examinar la amenaza, debemos preguntarnos constantemente qué es lo que el enemigo decidirá atacar, ya que no será necesariamente aeronaves en tierra. Los blancos y objetivos dependen de los atacantes, quienes pueden ser desde grupos terroristas hasta fuerzas convencionales y operaciones especiales, y de los objetivos políticos y la capacidad real que puedan utilizar contra la base aérea. En Vietnam, las fuerzas enemigas se dieron cuenta que los ataques terrestres contra los aeródromos representaban un drenaje de sus recursos. En consecuencia, se adaptaron a perturbar las operaciones aéreas en lugar de atacar directamente a los aeródromos, porque “si que las incursiones dañaban aeronaves, instalaciones o pistas de aterrizaje, el resultado era una disminución de las tasas de vuelo. Las armas de ataque a distancia [IDF en el léxico actual], así como otras formas de explosivos detonados por mando, pronto se convirtieron en las armas preferidas entre los muchos beligerantes involucrados en conflictos desde la década de 1960”.⁴

La amenaza del terrorismo ha dado lugar a que la mayoría de operaciones de defensa de la base se centren en derrotar a los dispositivos explosivos improvisados que se transportan en vehículos (VBIED). Los grupos terroristas principales siempre han querido realizar ataques espectaculares que causen muchas imágenes visuales, impacto traumático y alto número de muertos. Las imágenes del cuartel de la Infantería de Marina en Beirut, Líbano, o de las Torres Khobar de la Fuerza Aérea en Khobar, Arabia Saudita, se convirtieron en el resultado deseado de los ataques del adversario. Se ve la misma intención en la detonación de un camión explosivo del Talibán en el décimo aniversario de los ataques terroristas del 11 de septiembre de 2001, un ataque que hirió a 89 personas, incluyendo 77 soldados.⁵ Este artículo examina algunas de las amenazas más alarmantes—como los VBIED, que creemos que el enemigo usará en ataques futuros—y la tecnología emergente que podría permitirle atacar nuestras bases aéreas.

La creciente precisión del fuego indirecto

El IDF se ha convertido en la opción preferida entre los insurgentes para ataques a bases aéreas. Activado a distancia y con frecuencia manipulado para que se active después que el atacante se ha alejado, ofrece cierto grado de supervivencia. En Vietnam, las fuerzas norvietnamitas y del Vietcong atacaron las bases aéreas estadounidenses en 475 ocasiones entre 1964 y 1973, usando principalmente el IDF, destruyendo 99 aeronaves estadounidenses y survietnamitas, y dañando 1.170.⁶ En Irak, los insurgentes usaron el IDF para acosar a las bases aéreas, pero no fue eficaz debido al deficiente adiestramiento del enemigo y las defensas de base externas activas. En Afganistán el enemigo empleó el IDF no solo para acosar a las fuerzas de la coalición sino también para enmascarar y cubrir ataques de tierra. El 22 de agosto de 2012, las fuerzas enemigas se las arreglaron incluso para dañar el avión visitante del Presidente del Estado Mayor Conjunto.⁷

La efectividad de los morteros y cohetes, apuntados a una base por alguien que tiene información limitada del blanco, depende de la pericia técnica del operador—un factor que dificulta su eficacia total. Sin embargo, ha llegado una nueva era en sistemas de armas IDF de precisión. El 31 de marzo de 2011, los soldados de la Cuarta Brigada de Combate dispararon un proyectil de mortero con guía de precisión de 120 mm desde la Base de Operaciones de Avanzada de Kushamond, en Afganistán, impactando a unos cuatro metros del blanco.⁸ Normalmente un mortero dispara un proyectil “tonto”—que no tiene un sistema de guía integrado. Con el tiempo es probable que esta tecnología la adquieran los grupos insurgentes y terroristas, mejorando su capaci-

dad de elegir blancos con extraordinaria precisión y aumentando la vulnerabilidad de las aeronaves y las instalaciones importantes.

Para derrotar a este tipo de sistema de armas es necesaria una defensa tecnológica verdaderamente integrada. Tanto Estados Unidos como Israel han sido pioneros en sistemas defensivos diseñados para contrarrestar la creciente precisión de las armas IDF. En Irak, la Base Conjunta Balad y otras bases usaron un sistema de Mortero Anticohete manejado por personal conjunto para defenderse contra el IDF enemigo. En el futuro, el sector de defensa tendrá que asegurar un sistema de defensa completo porque los disparos de precisión harán que el ataque a una base sea más simple y las fuerzas defensoras tengan menos margen de error. Además, la capacidad de esta tecnología de defensa está mejorando. Por ejemplo, durante el conflicto israelí de noviembre de 2012 con Hamas en Gaza, los militantes lanzaron más de 1.500 cohetes contra Israel, pero la Cúpula de Acero (Iron Dome) de ese país, un “sistema anticohetes portátil desarrollado para derribar misiles de corto alcance”, interceptó unos 400 de ellos.⁹ Este sistema puede ofrecer un modelo de sistema de defensa portátil para operaciones aéreas. Si los disparos de IDF de precisión pasan a ser parte del entorno operativo, nuestros Aerotécnicos no tendrán el lujo de un enemigo incompetente que dispare proyectiles tontos.

Vehículos a control remoto

El personal que contemple la defensa de una base aérea debe considerar la amenaza que representan los vehículos a control remoto (RPV) mediante la formulación de un plan para enfrentar una gama de amenazas remotas, desde tierra y aerotransportadas. ¿Quién tiene autoridad para utilizar tales vehículos y con qué armas? Para vehículos basados en tierra, la respuesta está más claramente definida y concuerda con las contingencias establecidas para los VBIED; sin embargo, puede existir una brecha defensiva en la defensa contra las amenazas aerotransportadas. El hecho de que aún se tenga que explorar totalmente los protocolos para estas defensas deja una brecha que un enemigo con conocimientos tecnológicos podría explotar. Debemos desarrollar sistemas de modelado, simulación y defensa para tomar en cuenta las nuevas amenazas antes de que un grupo de protesta interrumpa las operaciones de vuelo o—peor aún—antes de que una organización terrorista utilice los RPV para reconocimiento o ataques contra nuestros activos aéreos.

El uso de estos vehículos (RPV, robots, vehículos teledirigidos, etc.) ya no se restringe al uso militar exclusivo. Después de todo, los civiles han volado aeroplanos a control remoto desde la década de 1930. Sin embargo, en la actualidad la sofisticación, el alcance y su capacidad de video permiten que los civiles accedan a tecnología que antes estaba reservada solo para organizaciones militares y de inteligencia. Pongamos el caso de un grupo de protesta denominado SHARK (Showing Animals Respect and Kindness) que propugna respeto y compasión por los animales. Este grupo planeó usar un Mikrokopter (vehículo teledirigido) para grabar un video de cómo se cazaban palomas vivas como medio de disuadir e interferir con una excursión de caza legal. El 21 de febrero de 2012, el grupo SHARK se instaló en Broxton Bridge Plantation cerca de Ehrhardt, Carolina del Sur. Agentes de la policía y un abogado local trataron de impedir que el grupo de protesta vuela su Mikrokopter, pero lo hicieron de todas maneras, solo para que lo derriben los cazadores en la escena.¹⁰

Esta misma tecnología es capaz de llevar armas o realizar reconocimiento para grupos que intenten atacar un aeródromo—de hecho, ya se ha hecho. Por ejemplo, aunque en años recientes los legisladores estadounidenses se han preocupado más por al-Qaeda, Hezbollah ha demostrado tener alcance global y capacidad de aguante. Es reconocido como el primer grupo terrorista en usar terroristas suicidas como arma de destrucción masiva, dirigiendo vehículos explosivos grandes a blancos estratégicos.¹¹ Hezbollah ha mostrado recientemente su destreza

tecnológica utilizando RPV con cargas explosivas y tecnología de misiles, logrando incluso incapacitar un barco de guerra israelí.¹² El éxito de la organización viene del respaldo financiero y logístico que recibe de Siria e Irán, éste último le suministra armas avanzadas y equipo de reconocimiento.

A partir de noviembre de 2004, Hezbollah asombró a los israelíes lanzando un avión de vigilancia a control remoto, el Misrad 1, que voló sobre poblados israelíes y volvió intacto a Líbano. En una manifestación de Hezbollah, el líder de la organización, Hassan Nasrallah, declaró, “Ustedes pueden cargar el avión Misrad con 40 ó 50 kilos de explosivos y enviarlo a su objetivo. . . . ¿Quieren una planta eléctrica, una planta de agua, una base militar? ¡Lo que sea!”¹³ Sin duda, con el tiempo, esta tecnología se difundirá a otros grupos terroristas y de protesta.

Para resaltar este punto, examinemos el caso de Rezwan Ferdaus, un ciudadano estadounidense de 26 años de edad. Fue arrestado el 28 de septiembre de 2011, acusado de planear el ataque al Pentágono y al Congreso Estadounidense con “aviones grandes a control remoto cargados con explosivo plástico C-4” y suministrar “apoyo material y recursos a una organización terrorista extranjera, específicamente a Al Qaeda”.¹⁴ Según la Oficina Federal de Investigaciones, Ferdaus planeaba complementar su “ataque aéreo” de tres vehículos teledirigidos con un ataque por tierra que incluía “seis personas armadas con armas automáticas divididas en dos equipos”. Ferdaus explicó que “con este ataque aéreo, podemos eliminar efectivamente lugares claves del edificio P [el Pentágono], después podemos añadir otras cosas para anular todo lo demás y dejar un área como lugar restringido solamente donde los individuos quedarían aislados, allí serán vulnerables y los podemos dominar”.¹⁵

Proliferación de misiles superficie-aire disparados desde el hombro

Un escuadrón de vuelo puede lograr éxito en la misión solo generando vuelos de aviones, sin importar las amenazas del entorno operativo. La protección de las aeronaves contra misiles SAM durante el despegue, la fase más vulnerable del vuelo, es sumamente difícil debido a las restricciones de maniobrabilidad causadas por el peso y la baja altitud. En consecuencia, las aeronaves de transporte pesado y su valiosa carga, posiblemente municiones y/o pasajeros, presentan blancos sumamente tentadores durante el despegue. Inversamente, los aviones que se aproximan tienen poco combustible y deben mantener velocidades y trayectorias de vuelo predecibles. En cualquiera de los dos casos, los misiles SAM representan una amenaza para tales aeronaves. Por ejemplo, los rebeldes en el actual conflicto sirio supuestamente poseen entre “quince y treinta sistemas de defensa aérea portátiles SA-7 [MANPADS]” y “aparentemente han derribado al menos cinco aeronaves de ala rotatoria y seis de ala fija”, cuando menos uno de ellos fue derribado por un MANPADS.¹⁶ De acuerdo con el Centro de la Fuerza Aérea de los Estados Unidos Contra la Proliferación,

Actualmente, 27 grupos terroristas, incluyendo Al Qaeda, han confirmado o reportado la posesión de MANPADS. Desde 1994, ha habido diez intentos de alto perfil para atacar aviones comerciales y se ha derribado cuatro, incluyendo uno que llevaba a los presidentes de Ruanda y Burundi. Además, los MANPADS se adaptan perfectamente al modo de operación de Al Qaeda y son relativamente fáciles de usar, de transporte conveniente, ampliamente disponibles, de poco costo, y definitivamente mortíferos.¹⁷

A medida que avanzan y proliferan las tecnologías desarrolladas por competidores extranjeros, las tácticas, técnicas y procedimientos para la defensa integrada tendrán que ponerse a la par con su empleo. Recientemente el MANPADS SA-24 “Grinch” de fabricación rusa pasó a Venezuela, Libia y Siria.¹⁸ Por cierto, el gobierno de Libia ha sido derrocado, y al momento de esta redacción Siria se mantiene en un estado de guerra civil. La seguridad de los MANPADS en los países en guerra es dudosa debido al potencial desarrollo de mercados negros y la inestabilidad que atrae elementos perversos. La amenaza de MANPADS para las fuerzas estadounidenses y de la coali-

ción, así como para las operaciones de las aerolíneas civiles probablemente aumentará a medida que estos sistemas se hagan más accesibles en el terreno fértil de la guerra civil y la insurgencia.

La creciente “amenaza interna”

En el futuro previsible, las fuerzas estadounidenses y de la coalición se desenvolverán en medio de amenazas internas. Desde 2007 hasta 2011 en Afganistán, las estadísticas del Pentágono revelan un total de 42 ataques realizados por miembros de las Fuerzas de Seguridad Nacional de Afganistán contra personal estadounidense o de la OTAN, causando la muerte de 70 soldados de la coalición e hiriendo a otros 110.¹⁹ Uno de los casos más graves y horribles de una amenaza interna ocurrió en la mañana del 27 de abril de 2011, cuando un capitán de la Fuerza Aérea Afgana asesinó a ocho aerotécnicos y un contratista en el Aeropuerto Internacional de Kabul.²⁰ Otro incidente demostró cómo un terrorista suicida decidido y astuto pudo infiltrar una base de la Agencia Central de Inteligencia (CIA) en el este de Afganistán y mató a ocho estadounidenses.²¹ Esta perturbadora tendencia se intensificó en 2012 cuando fuerzas de seguridad afganas uniformadas realizaron 46 ataques internos contra fuerzas de la coalición en las que perdieron la vida 60 miembros de la OTAN.²²

Aún más preocupante es la creciente amenaza dentro de las filas del personal estadounidense. El 11 de mayo de 2009, cinco de sus miembros militares fueron asesinados por un soldado estadounidense en un centro de consejeros en Camp Liberty, Bagdad.²³ En un tiroteo realizado por un psiquiatra del Ejército de los Estados Unidos el 5 de noviembre de 2009 en Fort Hood, Texas, resultaron muertas 13 personas y heridas otras 32.²⁴ Evidentemente, al Departamento de Seguridad Nacional le preocupa la amenaza que podrían crear los veteranos en el territorio nacional, teniendo en cuenta que éstos al volver de Irak y Afganistán podrían ser reclutados por los radicales de extrema derecha.²⁵

Es importante recordar que una persona puede causar un daño enorme, lo atestigua el número de incidentes “lobo solitario” que han ocurrido. Por ejemplo, el 22 de julio de 2011, Anders Breivik, un noruego, hizo explotar un coche bomba cerca de edificios del gobierno en Oslo, causando la muerte de ocho personas, y después masacró 69 personas en un campamento de jóvenes en la cercana isla de Utoeya.²⁶ El 20 de julio de 2012, el estadounidense James Holmes entró en un cine repleto de espectadores cerca de Denver y comenzó a disparar; asesinó a 12 e hirió a 58.²⁷ Los miembros militares estadounidenses capacitados y con experiencia y los veteranos podrían causar estragos aún mayores. Sea dentro del país o en ultramar, los comandantes deben asegurarse de proporcionar y ejecutar un plan de seguridad interior completo—uno que incluya un programa agresivo de evaluación psicológica para identificar las amenazas internas.

Obtención de mapas de las bases aéreas

Anteriormente, cuando las fuerzas enemigas planeaban un ataque terrestre contra una base aérea, se apoyaban en colaboradores con acceso a la base seleccionada para facilitar el mapeo del terreno y las instalaciones claves, y también para obtener distancias que hagan posible los ataques con fuego indirecto. Hoy, las autopistas de la información ofrecen acceso a imágenes satelitales y otras informaciones de dominio público que facilitan el trabajo del potencial atacante. Uno de esos sitios web, el de la Federación de Científicos Estadounidenses (FAS), se auto-describe como “un grupo de reflexión independiente, no partidario y registrado como organización con membresía sin fines de lucro 501(c)(3) . . . dedicado a proporcionar análisis rigurosos y objetivos basados en evidencia y recomendaciones de política práctica sobre asuntos de seguridad nacional e internacional conectados a la ciencia y tecnología aplicadas”.²⁸ GlobalSecurity.org, una ramificación de FAS fundada por John Pike, uno de sus ex miembros, se atribuye ser “la

fuerza principal de información de referencia y noticias recientes en los campos de defensa, espacio, inteligencia, armas de destrucción masiva [WMD], y seguridad nacional”.²⁹ Su sitio web contiene imágenes satelitales de bases militares alrededor del mundo, muchas de las cuales el gobierno estadounidense considera clasificadas. Otros sitios web, como Google Maps, ponen a disposición imágenes y mapas de calles. En resumen, ahora hay una multitud de formas de adquirir mapas detallados de bases aéreas que facilitarían ataques contra esas instalaciones.

Medios sociales: Turbas relámpago, terrorismo, y uso de la conexión en red para ataques a las bases

Las comunicaciones instantáneas mejorarán dramáticamente las operaciones de información del enemigo y los ataques a las bases, permitiéndoles aprovechar elementos favorables de una población local para crear situaciones que avergüencen al liderazgo de una base aérea o agobien las defensas. Por lo tanto, inteligencia y las autoridades policiales deben estar un paso por delante de un enemigo cada vez más ágil, mejorando la eficiencia de sus esfuerzos de recopilación de información. La tecnología básica, como los teléfonos celulares, ha afectado a la sociedad en formas insólitas creando medios sin precedentes para la comunicación y coordinación de las acciones. Pensemos por ejemplo el fenómeno en la “turba relámpago”, un grupo de gente convocada por teléfonos celulares, medios sociales y correos virales con el fin de realizar alguna clase de acto en un lugar específico. La Web e incluso los comerciales de las empresas de telecomunicaciones están repletos de imágenes de turbas relámpago benignas que aparecen en un lugar público para llevar a cabo alguna clase de acto inusual o artístico, como congelarse en un lugar o realizar una rutina de baile coordinado. Aunque hacen esto en nombre del entretenimiento, ¿qué sucede cuando alguien utiliza esta misma tecnología para fines nefastos?

En el verano de 2011, por ejemplo, en Filadelfia se produjo una epidemia de turbas relámpago organizadas para llevar a cabo robos, asaltos, saqueos, y caos. Este incidente incluyó golpizas a peatones al azar, alborotos en una tienda Sears, y reuniones de cientos de personas en lugares designados para estrangular el tráfico. Margaret Rock, editor de Multimedia.com en Chicago, dijo lo siguiente: “No se por qué, pero lo que comenzó como algo que se puede usar para el bien ha mostrado su lado oscuro”.³⁰ Posteriormente en ese mismo verano, ocurrieron disturbios en Londres, Birmingham, Manchester, y otros lugares, causando gran preocupación en los oficiales de seguridad. Scotland Yard identificó y arrestó cerca de 3.000 personas sospechosas de cometer excesos físicos o incitar a la violencia a través del país usando BlackBerry Messenger, Twitter, y Facebook.³¹ Según un texto, “Si quiere ganarse un dinero, estamos a punto de gastar mucho en el este de Londres”.³² David Cameron, Primer Ministro Británico, observó que “lo que observan estas acciones horribles quedarán sorprendidos al saber cómo se organizaron mediante los medios sociales. . . . Por eso estamos trabajando con la policía, los servicios de inteligencia y la industria para determinar si sería correcto impedir que estas personas se comuniquen por estos sitios web cuando sabemos que están tramando violencia, desorden y criminalidad”.³³

La rapidez del avance tecnológico ha llegado a todas las esquinas del mundo. Los teléfonos celulares son ahora potentes computadoras por derecho propio, conectándose en red con otros dispositivos de manera global. En ningún lugar es esto más evidente que en los países en desarrollo que tienen comunicaciones deficientes debido al costo de cablear la infraestructura para las líneas de tierra. Los teléfonos celulares le restan validez a ese gasto ya que las torres y los satélites permiten que esos países se conecten a la red global de comunicaciones. En 2008, el 80 por ciento de la población mundial tenía acceso a una red celular, y para fines de 2006, los países en desarrollo compraron el 68 por ciento de los teléfonos móviles del mundo.³⁴

La misma tecnología que habilita el intercambio y avance de la información global también permite la conexión en red de los grupos terroristas y criminales. Según un nuevo estudio de la Universidad de Haifa en Israel, Al-Qaeda, Hamas, Hezbollah, y otros similares han invertido en los medios sociales como Facebook y Twitter para reclutar, recolectar fondos y reunir inteligencia. El profesor Gabriel Wiemann, autor del estudio, sostiene que “en la actualidad, cerca del 90 por ciento del terrorismo organizado en Internet se lleva a cabo a través de los medios sociales” y que esto último está “permitiendo que las organizaciones terroristas tomen iniciativas haciendo pedidos de ‘amigos’, colgando videos cortos y similares, y ya no tienen que conformarse con las herramientas pasivas disponibles en los sitios web regulares”.³⁵

¿Cómo afectarán esta tecnología y las redes sociales a la seguridad de las bases en el futuro? Fácilmente se podría convocar a manifestantes, turbas y grupos terroristas sin previo aviso para la inteligencia militar o la policía, y reunirse rápidamente cerca del punto de entrada o el perímetro de una base para protestar, crear desórdenes o atacar. En muchos casos, tales áreas tendrían solo un puñado de vigilantes disponibles para contrarrestar a los grupos reunidos—un escenario que fácilmente podría abrumar al escaso personal en la escena e intensificarse más allá de su capacidad para sofocar tal acción.

Ciberataques: Un potencial “botón fácil” para ataque a una base aérea

Los avances tecnológicos han dado lugar a que los militares estadounidenses se apoyen en una “ciberfuerza” que depende principalmente de una red de computadoras y enlaces de comunicaciones, para asegurar no solo el uso efectivo de las fuerzas durante las operaciones de contingencia sino también la misión cotidiana de preparación y capacitación de la fuerza. Hasta ahora, los insurgentes han carecido de la capacidad y capacitación para llevar a cabo ciberataques en gran escala contra instalaciones militares. Sin embargo, es probable que eso cambie cuando las organizaciones terroristas auspiciadas por estados y las fuerzas insurgentes se asocien para derrotar a un enemigo común. La utilización de un ciberataque que afecte las operaciones aéreas o los sensores y cámaras de defensa de la base con el fin de facilitar un ataque cinético puede ser una opción económica y eficiente.

Los ataques a través del ciberespacio podrían degradar las operaciones de vuelo, tal como ocurrió en el Aeropuerto Internacional Indira Gandhi, cuando un código malicioso que utilizaba comandos específicamente diseñados para explotar la debilidad de ese sistema, desactivó los mostradores de facturación y las puertas de embarque afectando tremendamente las operaciones.³⁶ Un ataque similar podría interrumpir los nodos de control de tráfico aéreo, programas de mantenimiento en red, y operaciones de capacitación, y también amenazar a los RPV con armas o sin armas operados por la Fuerza Aérea y otras agencias del gobierno. Considere por ejemplo el reciente hackeo de un vehículo teledirigido del Departamento de Seguridad Nacional como parte de una apuesta entre un profesor de un instituto superior de Texas y sus alumnos. Con menos de \$1.000 dólares, estos individuos “engañaron” con éxito al RPV, “cambiándole efectivamente de misión”.³⁷ Esta broma académica de poco costo demuestra la facilidad con que un grupo adversario o terrorista podría cambiar de misión de los RPV y convertirlos en misiles volantes contra una base aérea u otro blanco.

Red Flag, el ejercicio de entrenamiento para combate de la Fuerza Aérea que incluye fuerzas estadounidenses y aliadas, ha integrado elementos cibernéticos y del espacio del Comando Espacial de la Fuerza Aérea para abordar efectos asociados con ataques contra activos cibernéticos o del espacio. En el ejercicio Red Flag de marzo de 2011, un oficial de la Fuerza Aérea comentó, “Sabemos de muchas amenazas alrededor del mundo que trabajan diligentemente para acceder, degradar o negarnos el uso de [sistemas de computadoras clasificados y no clasificados]”.³⁸ Los

activos y el personal asociado con los sistemas de defensa integrados pueden también convertirse en blancos. Además, los adversarios podrían intentar interrumpir o manipular el uso creciente del ciberespacio para las comunicaciones, incluyendo transmisiones de radio cifradas, mensajería clasificada y no clasificada, y sistemas de identificación biométrica en nuestras puertas de acceso. Una investigación del *Washington Post* encontró que ciertos tipos de plataformas de software usadas por el gobierno y el sector privado—incluyendo un sistema de la empresa Tridium llamado Niagara—son más vulnerables que otros. Marc Petock, vicepresidente para mercadeo y comunicaciones globales de Tridium, señaló que “algunas instalaciones del Departamento de Defensa en los Estados Unidos también dependen de Niagara. Eso incluye el gigantesco Almacén del Ejército de Tobyhanna en Pennsylvania” y algunas instalaciones militares de “alta seguridad”.³⁹

La rápida evolución del ciberdominio promete muchos beneficios: necesidad reducida de personal, mayor eficiencia, mejor selección de objetivos y facilidad de acceso/uso. No obstante, estas mismas tecnologías presentan importantes oportunidades para que un adversario ingenioso y determinado cree una puerta trasera a través de la cual puede penetrar e inutilizar la totalidad del sistema de seguridad.

Combinación de la tecnología moderna con las fuerzas especiales

No hace mucho tiempo, los planificadores en las bases de la OTAN se concentraban en los planes de la URSS para atacar bases aéreas. Durante la Guerra Fría, los soviéticos exploraron muchas formas de atacar e inhabilitar bases, principalmente empleando la Spetsnaz (fuerzas especiales). Una revisión de los perfiles de ataque contra aeródromos de la Spetsnaz en informes desclasificados de la Agencia Central de Inteligencia (CIA) del tiempo de la Guerra fría podría resultar útil porque ofrecen perspectivas sobre los métodos de ataque directo contra estos blancos. Estos incluían el lanzamiento en paracaídas de 30 operadores especiales en las cercanías de una base aérea, quienes se separarían en “cuatro equipos de operaciones, cada uno con responsabilidades específicas incluyendo capturar vehículos y personal con el fin de infiltrar el objetivo [base aérea]”, usando misiles SAM y dispositivos explosivos para destruir aeronaves.⁴⁰ Además,

en un segundo método, una compañía de Spetsnaz (aproximadamente 10 equipos de cinco a doce miembros) operaría contra un aeródromo fuertemente defendido. La compañía no podía acercarse a menos de 2 ó 3 kilómetros del objetivo. Durante la primera noche situarían Block Strelas [lanzamisiles SAM de tres tubos montados en trípode] lo más cerca posible de uno de los extremos del campo, y después se iniciarían ataques contra sistemas de tuberías, líneas de transmisión, líneas de comunicación, personal de seguridad, y las cuadrillas que se dirigían al aeródromo.⁴¹

Esto interrumpiría las operaciones del aeródromo, crearía la impresión de que había una fuerza soviética más grande en el área, y atraería más tropas de la OTAN para la defensa y lejos de las líneas de fuego. Imagínense fuerzas especiales enemigas bien capacitadas que dispongan de muchos de los avances tecnológicos antes mencionados. La defensa de la base se volvería increíblemente difícil, y la complejidad del contrarresto de la amenaza aumentaría significativamente.

Conclusión

El entendimiento y contrarresto de estas crecientes amenazas jugará un papel muy importante en la capacidad de proyectar poderío aéreo de forma efectiva en el futuro. Una solución—poner la base de las aeronaves lo más lejos posible de las hostilidades—impone en las aeronaves y sus tripulaciones tiempos de vuelo más largos. Sin embargo, esto no resuelve el requisito probable de que las aeronaves de movilidad aterricen cerca de o en la zona de combate para apoyar las operaciones de tierra. Ni tampoco las bases remotas responden a los medios tecnológicos de ataque a través del ciberespacio, terroristas tecnológicamente habilitados, o fuerzas especiales

que atacan una base aérea supuestamente segura. Por lo tanto, los Aerotécnicos deben realizar un verdadero análisis de amenaza de espectro total y tomar en consideración estas potenciales vulnerabilidades en el planeamiento de protección de la fuerza.

Las aeronaves son sumamente frágiles. Un proyectil de mortero bien puesto puede inutilizar aeronaves por valor de varios cientos de millones de dólares o destruir las barracas ocupadas por personal esencial, como pilotos o técnicos de aeronaves. Las fuerzas de la Fuerza Aérea y de la coalición tendrán que tomar decisiones difíciles sobre defensa de la base teniendo en cuenta los requisitos de la misión, las restricciones económicas, y la creciente amenaza que presenta un enemigo decidido habilitado por alguna de las tecnologías antes mencionadas. Los Aerotécnicos y los líderes conjuntos deben mantenerse al tanto de estos problemas durante el período entre guerras o arriesgar la eliminación y degradación de los activos aéreos al comienzo de la próxima campaña importante. □

Notas

1. Barbara Starr, Chris Lawrence y Joe Sterling, "ISAF: Insurgentes en ataque mortal en Afganistán vestían uniformes del ejército de los Estados Unidos", Cable News Network, 15 de septiembre de 2012, <http://www.cnn.com/2012/09/14/world/asia/afghanistan-fatal-attack/index.html>.

2. Giulio Douhet, *The Command of the Air (El Comando del Aire)*, trans. Dino Ferrari (1942; nueva impresión, Washington, DC: Oficina de Historia de la Fuerza Aérea, 1983), 53–54.

3. James S. Corum y Wray R. Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists (Poderío Aéreo en las Guerras Menores: Combatiendo a Insurgentes y Terroristas)* (Lawrence: University Press of Kansas, 2003), 334–35.

4. Mayor Michael P. Buonaugurio, USAF, "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision (Defensa de la base aérea en el siglo 21: Fuerzas de seguridad de la USAF protegen el aspecto de la visión conjunta)" (tesis de maestría, Marine Corps Command and Staff College, 2001), 8, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA401262>.

5. Jeremy Kelly, "Base militar de la OTAN atacada por terrorista suicida en Afganistán," *Guardian*, 11 de septiembre de 2011, <http://www.guardian.co.uk/world/2011/sep/11/us-base-suicide-bomber-afghanistan>.

6. Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases (Serpientes en el Nido del Ágila: Una Historia de los Ataques Terrestres Contra Bases Aéreas)* (Santa Monica, CA: RAND, 1995), 68, http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR553.pdf.

7. Barbara Starr, "Esquirlas impactan avión del Presidente del Estado Mayor en una base afgana" Cable News Network, 21 de agosto de 2012, http://articles.cnn.com/2012-08-21/asia/world_asia_afghanistan-dempsey-plane_1_fight-against-afghan-green-on-blue-afghan-man-afghanistan.

8. Sargento Tercero Todd Christopherson, "Soldados disparan el primer mortero con guía de precisión en Afganistán", Ejército de los Estados Unidos, 7 de abril de 2011, <http://www.army.mil/article/54502/>.

9. Jennifer Rizzo, "Estados Unidos continúa apoyando la cúpula de acero de Israel", Cable News Network, 17 de mayo de 2012, http://articles.cnn.com/2012-05-17/us/us_israel-missile-system_1_anti-rocket-iron-dome-missile-defense?s=PM:US; y Ernesto Londoño, "Para Israel, el sistema de defensa contra misiles Cúpula de Acero representa un gran avance", *Washington Post*, 2 de diciembre de 2012, http://www.washingtonpost.com/world/national-security/for-israel-iron-dome-missile-defense-system-represents-breakthrough/2012/12/01/24c3dc26-3b32-11e2-8a97-363b0f9a0ab3_story_1.html.

10. Rebecca Boyle, "Después que activistas hacen seguimiento con vehículo teledirigido de caza de palomas, los cazadores de palomas lo derriban," *Popular Science*, 21 de febrero de 2012, <http://www.popsci.com/technology/article/2012-02/after-pigeon-hunt-thwarted-shooters-take-down-activist-groups-spy-drone>.

11. Capitán Daniel Helmer, "Hezbollah's Employment of Suicide Bombing during the 1980s: The Theological, Political, and Operational Development of a New Tactic (Empleo de terroristas suicidas por Hezbollah durante la década de 1980: El desarrollo teológico, político y operativo de una nueva táctica)", *Military Review*, Julio-Agosto de 2006, http://www.army.mil/professionalWriting/volumes/volume4/november_2006/11_06_1.html.

12. Associated Press, "Israel: Tropas iraníes ayudan en ataque de Hezbollah", *NBC News*, 16 de julio de 2006, <http://www.nbcnews.com/id/13875121/>.

13. Lisa Myers, "Vehículo teledirigido de Hezbollah amenaza a Israel", *NBC News*, 12 de abril de 2005, <http://www.msnbc.msn.com/id/7477528/ns/nbcnightlynews/t/hezbollah-drone-threatens-israel/>.

14. "Residente de Massachusetts es acusado de planear ataque contra el Pentágono y el Capitolio de Estados Unidos e intentar el suministro de apoyo material a una organización terrorista extranjera", comunicado de prensa, Oficina

Federal de Investigaciones, 28 de septiembre de 2011, <http://www.fbi.gov/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization>.

15. *Ibíd.*

16. Eddie Boxx y Jeffrey White, “Respuesta al uso del poderío aéreo de Assad en Siria”, 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>.

17. James C. “Chris” Whitmire, *Shoulder Launched Missiles (a.k.a. MANPADS): The Ominous Threat to Commercial Aviation (Misiles disparados desde el hombro (o MANPADS): La ominosa amenaza contra la aviación comercial)*, Documentos Contra la Proliferación, Serie Future Warfare No. 37 (Maxwell AFB, AL: Centro de la Fuerza Aérea de los Estados Unidos Contra la Proliferación, Universidad del Aire, diciembre de 2006), 1, <http://cpc.au.af.mil/PDF/monograph/manpads.pdf>.

18. David Fulghum y Robert Wall, “SA-24 ‘Grinch’ de Rusia cae en manos insurgentes”, *Aviation Week and Space Technology*, 12 de marzo de 2012, http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_03_12_2012_p27-433282.xml&p=1.

19. Anna Mulrine, “¿Infiltrados del Taliban en Afganistán? El Pentágono advierte sobre la ‘amenaza interna’”, *Christian Science Monitor*, 1 de febrero de 2012, <http://www.csmonitor.com/USA/Military/2012/0201/Taliban-infiltrators-in-Afghanistan-Pentagon-warns-of-insider-threat>.

20. Jill Laster, “Motivo del tiroteo de Kabul sigue siendo esquivo”, *Air Force Times*, 17 de enero de 2012, <http://www.airforcetimes.com/news/2012/01/air-force-motive-in-kabul-shooting-deaths-remains-elusive-011712/>.

21. Joby Warrick, “Terrorista suicida ataca base de la CIA en Afganistán, dando muerte al menos a 8 estadounidenses”, *Washington Post*, 31 de diciembre de 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/30/AR2009123000201.html>.

22. “¿Qué hay detrás de los ataques internos en Afganistán?”, British Broadcasting Corporation, 11 de marzo de 2013, <http://www.bbc.co.uk/news/world-asia-19633418>.

23. Timothy Williams, “Soldado estadounidense asesina a 5 de sus compañeros en Irak”, *New York Times*, 11 de mayo de 2009, http://www.nytimes.com/2009/05/12/world/middleeast/12iraq.html?_r=2.

24. Joseph I. Lieberman y Susan M. Collins, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack (Una bomba de tiempo: Lecciones antiterrorismo de la falla del gobierno de los Estados Unidos para prevenir el ataque de Fort Hood)*, informe especial (Washington, DC: Comisión del Senado de los Estados Unidos sobre Seguridad Nacional y Asuntos del Gobierno, febrero de 2011), <http://www.hsgac.senate.gov/download/fort-hood-report>.

25. Associated Press, “Líderes de Seguridad Nacional defienden memo sobre veteranos de guerra”, *USA Today*, 19 de abril de 2009, http://usatoday30.usatoday.com/news/washington/2009-04-19-homeland-memo_N.htm.

26. “Anders Breivik describe la masacre en isla de Noruega”, BBC, 20 de abril de 2012, <http://www.bbc.co.uk/news/world-europe-17789206>.

27. M. Alex Johnson y Pete Williams, “Policía: Se realizaron semanas de planeamiento para los tiroteos en la proyección de Batman en Colorado”, *NBC News*, 20 de julio de 2012.

28. “Acerca de la FAS”, Federación de Científicos Estadounidenses, consultado el 29 de enero de 2013, <https://www.fas.org/about/index.html>.

29. “Historia de la empresa”, GlobalSecurity.org, consultado el 13 de marzo de 2013, <http://www.globalsecurity.org/org/overview/history.htm>.

30. John Timpane, “Violencia de las turbas relámpago levanta preguntas importantes”, Philly.com, 14 de agosto de 2011, http://articles.philly.com/2011-08-14/news/29886718_1_social-media-flash-mob-facebook-and-other-services.

31. Neil Lancefield, “3,000 arrestos en investigación de disturbios en Londres”, *Independent*, 7 de octubre de 2011, <http://www.independent.co.uk/news/uk/crime/3000-arrests-in-london-riots-investigation-2366933.html>.

32. Timpane, “Violencia de las turbas relámpago”.

33. Josh Halliday, “David Cameron considera prohibir que los agitadores sospechosos entren en los medios sociales”, *Guardian*, 11 de agosto de 2011, <http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media>.

34. Sara Corbett, “¿Puede el teléfono celular ayudar a terminar con la pobreza global?”, *New York Times*, 13 de abril de 2008, <http://www.nytimes.com/2008/04/13/magazine/13anthropology-t.html?pagewanted=all>.

35. “Grupos terroristas utilizan los medios sociales para reclutar”, Canadian Broadcasting Corporation News, 10 de enero de 2012, <http://www.cbc.ca/news/technology/story/2012/01/10/tech-terrorist-social-media.html>.

36. Rahul Tripathi, “Ciberataque dio lugar a la paralización del Aeropuerto Indira Gandhi”, *Indian Express*, 25 de septiembre de 2011, <http://www.indianexpress.com/news/cyber-attack-led-to-igi-shutdown/851365/>.

37. “Instituto Superior de Texas hackea vehículo teledirigido del gobierno frente al Departamento de Seguridad Nacional”, Organización autónoma sin fines de lucro (“TV-Novosti”), 27 de junio de 2012, <http://rt.com/usa/news/texas-1000-us-government-906/>.

38. Sargento Segundo Scott McNabb, “Red Flag Cyber Operations: Part I—Isn’t Red Flag a Flyer’s Exercise? (Operaciones cibernéticas Red Flag: Parte I—¿No es Red Flag un ejercicio de vuelo?)”, Comando Espacial de la Fuerza Aérea, 1 de marzo de 2011, <http://www.afspc.af.mil/news/story.asp?id=123244481>.

39. Robert O’Harrow Jr., “Tridium’s Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks (Marco teórico de Niagara de Tridium: Maravilla de conectividad ilustra nuevos riesgos cibernéticos)”, *Washington Post*, 11 de julio de 2012, http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html.

40. Director de Inteligencia Central, *Warsaw Pact Nonnuclear Threat to NATO Airbases in Central Europe (Amenaza no nuclear del pacto de Varsovia para las bases aéreas de la OTAN en Europa Central)*, NIE 11/20-6-84, 25 de octubre de 1984, 35, http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000278545.pdf. Este documento ha sido desclasificado.

41. *Ibid.*, 36, 39.



El Coronel Shannon W. Caudill, USAF (BS, Norwich University; MS, Central Michigan University; MMS, Marine Corp University) es estudiante en el Programa de Gran Estrategia de la Escuela Superior de Guerra de la Fuerza Aérea y ex vicepresidente del Departamento de Liderazgo y Estrategia, Escuela Superior de Comando y Estado Mayor, Base Aérea Maxwell, Alabama. Antes de ocupar su puesto actual, el Cnel. Caudill estuvo al mando del 532º Escuadrón Expedicionario de Fuerzas de Seguridad (los Leones), Base Conjunta Balad, Irak. En calidad de oficial de carrera en las fuerzas de seguridad, se ha desempeñado a niveles de unidad, comando principal y estado mayor conjunto; ha estado al mando de tres escuadrones de fuerzas de seguridad; servido en cuatro asignaciones en ultramar y acumulado 18 horas de experiencia en combate en Irak. El Cnel Caudill ha escrito varios informes blancos y artículos sobre terrorismo, liderazgo interinstitucional y cumplimiento de la ley que han sido publicados en el *Air and Space Power Journal*, *Joint Force Quarterly*, *American Diplomacy* y *The Guardian*—la publicación sobre antiterrorismo del Estado Mayor Conjunto. El Coronel es egresado de la Escuela Superior para Oficiales de Escuadrón, de la Escuela Superior de Comando y Estado Mayor del Cuerpo de Infantería de Marina y de la Escuela Superior de las Fuerzas Conjuntas.



El Mayor Benjamin R. Jacobson, USAF (BS, University of Idaho; MBA [con énfasis en Justicia Criminal], Touro University; MMOAS, Escuela Superior de Comando y Estado Mayor) es director adjunto del Curso de Estudios Aéreos, Espaciales y de Poder Cibernético, Departamento de Liderazgo y Estrategia, Escuela Superior de Comando y Estado Mayor, Base Aérea Maxwell, Alabama. Antes de ocupar su puesto actual, el Mayor Jacobson estuvo al mando del 96º Escuadrón de Entrenamiento en Combate Terrestre, Base Aérea Eglin, Florida. En calidad de oficial de carrera en las fuerzas de seguridad, el Mayor Jacobson se ha desempeñado a niveles de unidad, ala y comando principal y ha servido en dos asignaciones en ultramar. El Mayor Jacobson es egresado del Curso Básico Aeroespacial, de la Escuela Superior para Oficiales de Escuadrón y de la Escuela Superior de Comando y Estado Mayor.