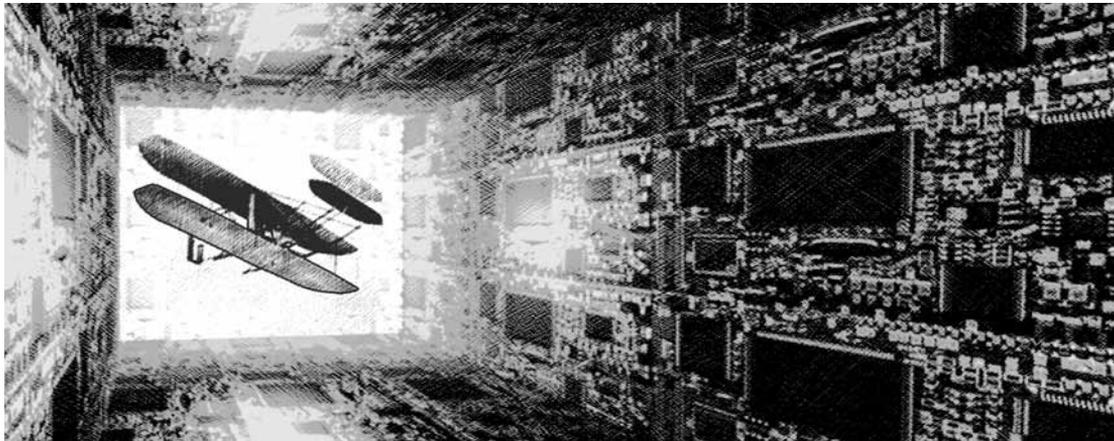


Ciber Esto, Ciber Aquello... ¿Y Qué?

MAYOR (USAF) ERIC D. TRIAS, PHD

CAPITÁN (USAF) BRYAN M. BELL



Para comprender el presente, hay que conocer el pasado

—Carl Sagan

LAS REVOLUCIONES en la guerra rara vez tienen lugar durante nuestras vidas. En cambio, una evolución basada en el uso innovador de la tecnología disponible y la ingeniosidad humana ocurre constantemente.¹ ¿Acaso la ubicuidad de las operaciones ciberespaciales y la tecnología es esa revolución? Quizás. Sin embargo, ninguna revolución nos debe obligar a dejar atrás las lecciones aprendidas de la era antes del ciberespacio. Estudiantes asiduos de la guerra aún opinan que los libros sobre historia militar, teorías de guerra, doctrinas y publicaciones sobre conflictos pasados son de un valor incalculable. Desde el punto de vista del caballero del aire, el ciberespacio no cambia los principios de guerra o del poderío aéreo. A un nivel aún más granular, solamente se requieren efectuar cambios menores a las misiones aéreas y espaciales (y ciberespaciales) de la Fuerza Aérea de Estados Unidos.

Cuando el jefe de estado mayor y el secretario de la Fuerza Aérea agregaron el ciberespa-

cio al enunciado de la misión del servicio en diciembre de 2005, se tornó evidentemente claro que la Fuerza Aérea hablaba en serio acerca de su función en proveerle a la guerra conjunta capacidades en las operaciones ciberespaciales.² Como resultado, la comunidad de la Fuerza Aérea, junto con sus homólogos en los demás servicios armados, ha estado ocupada redactando documentos de apoyo y orientación para definir y enfocar lo que el área de la misión en ciernes significa para la fuerza. El ciberespacio se encuentra en todas partes; forma parte esencial de nuestra misión y actividades diarias. No obstante, debemos recordar que nuestras funciones fundamentales como Fuerza Aérea no han cambiado.

En este artículo se apoya la idea que las operaciones ciberespaciales se pueden llevar a cabo en todos los ámbitos de la guerra: Aérea, espacial, ciberespacial, terrestre y marítima. Además, a pesar de la inmadurez de las doctrinas ciberespaciales operacionales, las doctrinas aérea y espacial permanecen vigentes y

pertinentes al ámbito ciberespacial. Las operaciones ciberespaciales no son tan sólo otro conjunto de herramientas en el estuche de herramientas del comandante. Aunque las operaciones ciberespaciales tienen maneras singulares de lograr efectos, desde la perspectiva de la Fuerza Aérea son similares a otras operaciones aéreas y espaciales que apoyan las misiones aéreas y espaciales (y ciberespaciales). Las operaciones ciberespaciales conocidas y establecidas les ofrecen a los guerreros opciones viables a medios cinéticos. En este artículo se destaca el papel que desempeñan las operaciones ciberespaciales para apoyar las misiones aérea y espacial.

Por último, a las misiones de la 17ª Fuerza Aérea le agregamos una nueva misión, *contraciberespacial*, (consulte la tabla). La doctrina anterior de la Fuerza Aérea ha empleado una nomenclatura diferente pero no fue sino hasta recientemente que aclaró completamente la importancia del contraciberespacio. Por este motivo, la nueva misión exige ajustes a la misión existente de las operaciones de información (IO) para justificar la duplicación. Al mostrar que las operaciones ciberespaciales son tan sólo otro conjunto de herramientas, podemos integrar operaciones de apoyo anteriormente definidas en una elaboración inicial de la doctrina de las operaciones ciberespaciales. Posiblemente, una doctrina ciberespacial más concreta evolucionará según la dicten las lecciones de la historia y los eventos futuros.

La doctrina es una colección integrada de lecciones aprendidas de experimentos, ejercicios y enfrentamientos anteriores que aceptamos como las *mejores prácticas* para llevar a cabo la guerra.³ Aún en su etapa inicial, las operaciones ciberespaciales, por consiguiente, carecen la historia de la experiencia vital para establecer enunciados de doctrina firmes. El Dr. David Lonsdale comentó que “los métodos de guerra, nuevos o por crearse, requieren un desarrollo de doctrina y teórico que se basen en, y sean informados por, la experiencia, conocimiento histórico y las obras de teóricos universales, especialmente Carl von Clausewitz y Sun Tzu”.⁴ Los estrategas de la Fuerza Aérea están luchando por crear principios de doctrina para la guerra ciber-

espacial en la forma del Documento de Doctrina de la Fuerza Aérea (AFDD) 2-11, “*Operaciones Ciberespaciales*”, que ya lleva varios años en redacción. Sin embargo, debemos tener cuidado de derivar la doctrina y la estrategia ciberespacial de los métodos comprobados extraídos de documentos anteriores y debemos analizar cómo podemos emplear las operaciones ciberespaciales en apoyo a las misiones de la Fuerza Aérea.

Las misiones de la Fuerza Aérea definidas en el AFDD 1, *Doctrina Básica de la Fuerza Aérea*, son aquellas responsabilidades específicas que le permiten al servicio cumplir con sus funciones establecidas legalmente según se estipula en el Título 10, *Código de Estados Unidos*, Sección 88013. Las funciones operacionales que ilustradas en la tabla anterior son “actividades amplias, básicas y en curso” del poder aéreo, espacial y ciberespacial.⁵ “No son necesariamente exclusivamente de la Fuerza Aérea...pero juntas sí representan” cómo el servicio cumple con las misiones que se le asignan.⁶ En las siguientes secciones se tratan cada una de las funciones aéreas y espacial, discutiendo cómo las operaciones ciberespaciales pueden proveer los mismos efectos y sirven como la base correcta para la doctrina ciberespacial.

Ataque Estratégico

La meta del ataque estratégico es aplicar la fuerza sistemáticamente contra los centros de gravedad del enemigo para poder producir el mayor efecto al menor costo posible en dólares y vidas.⁷ Tal como lo ilustran los cinco anillos estratégicos de Warden, esos centros pueden ser materiales (infraestructura) o no materiales (apoyo de la población) en naturaleza. Además, él aboga por atacar los tres elementos de mando, recopilación de información, toma de decisiones y comunicaciones (por ejemplo, bombardear la infraestructura de comunicaciones de Irak durante la Operación Tormenta en el Desierto, tal como se mostró en la Cadena de Noticias por Cable (CNN)).⁸

El ámbito ciberespacial les provee a los adversarios un nuevo entorno para llevar a cabo operaciones ofensivas y defensivas. Además,

Tabla. Misiones aéreas, espaciales y ciberespaciales de la Fuerza Aérea

<i>Misión</i>	<i>Definición General</i>	<i>Ejemplo Aéreo y Espacial</i>	<i>Tareas Ciberespaciales</i>
Ataque estratégico	Aplicación sistemática de la fuerza contra los centros de gravedad del enemigo	Destruir liderazgo, poder y los centros de comunicación	Ataque, control de supervisión y adquisición de datos y tráfico en la Internet
Contraaire, Contraespacio, Contratierra, ContraMarítimo	Operaciones llevadas a cabo para lograr y mantener un grado deseado de superioridad dentro de un ámbito a la vez que se le niega al adversario el uso de ese mismo ámbito	Interdicción aérea, apoyo aéreo cercano, supresión de las defensas aéreas del enemigo, interferencia de las frecuencias de satélite ascendente/descendente	Manipular bases de datos, imágenes, potencia/ controles de un sistema de armamento
Operaciones de Información	Medidas para apoyar la capacidad de los comandantes de evaluar el entorno operacional y mejorar su circuito de observar-orientar-decidir-actuar	Operaciones de influencia, guerra electrónica, engaño militar, contrainteligencia	Manipulación del contenido de la red, "volantes" por correo electrónico
Transporte aéreo, reaprovisionamiento de combustible, transporte espacial	Actividades que extienden el alcance del personal y pertrechos para ofrecer opciones rápidas, que funcionales, flexibles, oportunas y responsivas	Transporte aéreo dentro del teatro, transporte aéreo de apoyo operacional, lanzamiento de despliegue	Mensajes por correo electrónico, páginas Web, administración a distancia de la red
Inteligencia, vigilancia y reconocimiento	Actividades que contribuyen a la creación de la preparación de inteligencia del espacio de batalla para poder ofrecerles a los comandantes conocimientos detallados que los ayuden a comprender y conocer mejor al enemigo	U-2, aviones piloteados por control remoto, recursos nacionales, inteligencia humana	Buscadores, enumeración de la red, <i>honeypots</i> , <i>packet sniffing</i>
Operaciones especiales	Operaciones que usan movilidad en territorio negado, potencia de fuego quirúrgica y tácticas especiales para llevar a cabo acciones militares de baja visibilidad, encubiertas o clandestinas	Reconocimiento especial, operaciones psicológicas, contraterrorismo	Enmascarar direcciones, cibercafé, <i>botnets</i>
Apoyo de combate, mando y control, búsqueda y rescate de combate, navegación y posicionamiento, servicios meteorológicos	Acciones que le permiten al guerrero enfocarse y llevar a cabo con éxito aquellas operaciones relacionadas con las funciones mencionadas anteriormente	Mantenimiento de aeronaves, centro de operaciones aéreas y espaciales, satélites de sistema de posicionamiento global, satélites de la Administración Nacional Oceánica y Atmosférica	Operaciones centradas en la red, mando y control y paquetes de terreno en la red
Contraciberespacial	Operaciones que se llevan a cabo para lograr y mantener cierto grado de superioridad ciberespacial al destruir, degradar, negar, engañar, interrumpir o explotar la capacidad ciberespacial del enemigo	Bombardear edificios que alojan servidores	Explotación de software

las operaciones ciberespaciales ofrecen un medio para agilizar otras funciones operacionales llevadas a cabo anteriormente a través de otros ámbitos. “En el intento de influenciar, ya sea enfocándose en un individuo, una organización o toda una sociedad, el ciberespacio es un medio operacional clave mediante el cual se lleva a cabo la ‘influencia estratégica’”.⁹ No obstante, tomando en cuenta la dependencia de las organizaciones modernas y de las naciones en la infraestructura ciberespacial del mundo, nuevas fuentes de vulnerabilidades son blancos tentadores para el ataque estratégico, especialmente desde el punto de vista de una guerra asimétrica.

Durante los últimos años, la capacidad para poder usar las operaciones ciberespaciales como una vía para el ataque estratégico se ha tornado evidente. En el 2007, el Laboratorio Nacional de Idaho del Departamento de Seguridad Interna simuló un ataque ciberespacial en una central eléctrica de prueba. La simulación demostró una explotación de una vulnerabilidad del *software* en los sistemas de Control de Supervisión y Registro de Datos (SCADA), los sistemas de computadoras que controlan las plantas de energía eléctrica, de agua y químicas en Estados Unidos. Concebidos con una protección de seguridad mínima, muchos de estos sistemas permanecen vulnerables a los ataques cibernéticos. Inclusive las organizaciones terroristas están interesadas en las vulnerabilidades de los sistemas estratégicos tales como SCADA.¹⁰ Ejemplos incluyen un cierre virtual del gobierno estonio vía su infraestructura de la Internet y el conflicto entre Rusia y Georgia en el 2008, durante el cual las fuerzas militares rusas orquestaron una ola de operaciones relacionadas con la cibernética contra Georgia antes de la invasión. Coordinado a través de un foro ruso en línea, el asalto en línea pareció estar preparado con listas de blancos y detalles acerca de las vulnerabilidades. Los ataques cibernéticos se llevaron a cabo antes de que los dos países se enfrentaran en una guerra terrestre, marítima y aérea que duró cinco días.¹¹

Contra-aire, Contra-espacio, Contra-tierra, Contra-marítimo

Estas operaciones se llevan a cabo para “lograr y mantener un grado de superioridad deseado” dentro de cualesquier ámbito físico destruyendo, degradando, negando, engañando, interrumpiendo y explotando la capacidad del enemigo dentro del mismo ámbito.¹² Se caracterizan por medidas que son ofensivas o defensivas en naturaleza. Las contraoperaciones de ofensiva le impiden al enemigo explotar a su favor un ámbito en particular.¹³ Una meta de las operaciones contraaire ofensivas tiene que ver con destruir los recursos aéreos y los misiles de ofensiva del enemigo antes de que él pueda hacer lo mismo para poder establecer libertad de ataque de las fuerzas amigas. Las contraoperaciones defensivas “preservan la capacidad de EE.UU./aliados de explotar” un ámbito para poder proteger las capacidades amigas.¹⁴ Durante la Operación Libertad para Irak, las fuerzas de la Coalición llevó a cabo una operación contraespacial defensiva para destruir los “interruptores del sistema de posicionamiento global (GPS) en tierra del adversario para conservar la libertad de que las fuerzas amigas pudiesen emplear las municiones guiadas por GPS”.¹⁵

Los recursos militares de Estados Unidos a lo largo de todos los ámbitos operacionales están repletos de tecnologías cibernéticas, como es el caso en la mayoría de las milicias modernas. En el *Quadrennial Roles and Missions Review Report* (Informe trimestral de revisión de funciones y misiones) se esboza el deseo de Departamento de Defensa de buscar “capacidades ciberespaciales estratégicas, operacionales y tácticas para proveer . . . efectos bélicos dentro y a través del ámbito ciberespacial que son sinérgicos con los efectos dentro de otros ámbitos”.¹⁶ Las herramientas y operaciones relacionadas con el ciberespacio se han tornado comunes, por no decir prerequisites, en las operaciones militares. Sistemas tales como los enlaces de datos compartidos entre las plataformas y los centros de mando y control (C2), el *Blue Force Tracker* que utiliza el Ejército de EE.UU y las tecnologías de aterrizaje en portaaviones ayudadas por GPS utiliza-

das por la Armada de EE.UU. han cambiado la ejecución de operaciones específicas. Sin embargo, existen para apoyar las funciones del mismo servicio.

Los *hackers* ya han dado muestras de su capacidad de entrar en las redes del DoD y de los contratistas.¹⁷ Lograr acceso a las bases de datos de C2 en la Internet presenta una oportunidad para afectar la coordinación de lanzar fuerzas desde la guarnición, la dirección que toman y sus acciones al llegar. Una brecha exitosa en las arquitecturas de comunicación/enlace de datos de un sistema de armamento fácilmente nos permitiría interrumpir la capacidad del enemigo de llevar a cabo su misión. La infiltración a los sistemas habilitados por la cibernética del enemigo también nos permitiría manipular su situación operacional o influenciar la entrega de energía eléctrica o el funcionamiento de los sistemas de control por satélite.

Operaciones de Información

Según se define en el AFDD 2-5, Operaciones de Información (IO), las mismas existen para apoyar a los comandantes a definir la situación, evaluar las amenazas y los riesgos y tomar decisiones oportunas y correctas. Dependiendo de la información precisa y su velocidad de recorrido hace que el espectro de información sea más importante que nunca. En la actualidad, las IO consisten en operaciones de influencia, operaciones de guerra en la red y operaciones de guerra electrónica (EW).¹⁸ Con la llegada de las operaciones ciberespaciales, está claro que las operaciones de guerra en la red caen bajo este nuevo concepto. Sin embargo, continúa un debate sobre el futuro de la EW. Después de la publicación de una doctrina para las operaciones ciberespaciales, el AFDD 2-5 se debe revisar para incorporar esos cambios.

Esto no significa que las dos son mutuamente exclusivas. Las IO se pueden llevar a cabo en el ámbito ciberespacial, como ha sucedido por décadas en otros ámbitos operacionales. No obstante, no todas las IO se pueden considerar operaciones ciberespaciales. Por

ejemplo, las operaciones de influencia buscan lograr efectos que resultan en un cambio en el circuito observar, orientar, decidir y actuar del enemigo. Los medios tradicionales incluyen lanzar volantes o utilizar mensajeros humanos para llevar a cabo las operaciones psicológicas (PSYOP). Las operaciones EW buscan lograr efectos a lo largo del ámbito electromagnético, inclusive frecuencias de radio al igual que las regiones ópticas e infrarrojas del espectro. Las operaciones EW tradicionales llevadas a cabo por las tripulaciones durante los últimos cincuenta años son consideradas operaciones no cibernéticas por comunidades enteras.¹⁹ “En la Operación Fuerza Aliada ... las capacidades de muchos servicios fueron combinadas en la forma de ‘interrumpir para explotar’, demostrando cómo los usuarios de las comunicaciones del oponente se pueden encaminar a frecuencias que la inteligencia puede recopilar y explotar”.²⁰ A menudo, las IO consisten en acciones no cinéticas para defender nuestro ciclo de decisión e influenciar el del adversario, pero también pueden adoptar la forma de un ataque físico contra infraestructuras de información tangibles.

Las actividades de contrainformación de ofensiva de las PSYOP, el engaño militar y el ataque a la información todos tienen un lugar en el ámbito cibernético. Fuerzas cibernéticas bien adiestradas pueden influenciar los ciclos de decisión del enemigo al presentarles contenido engañoso de una Web o inclusive cambiar información presentada por fuentes acreditadas. Las actividades de contrainformación de defensiva tales como la garantía de la información y los protocolos de seguridad operacional ya están disponibles en todas las instalaciones de la Fuerza Aérea, algunas en forma no cibernética.

Transporte aéreo, reaprovisionamiento de combustible en vuelo y transporte espacial

El transporte aéreo, el reaprovisionamiento de combustible en vuelo y el transporte espacial extienden el alcance del personal y los pertrechos para ofrecer opciones rápidas, que

funcionan, flexibles, oportunas y responsivas necesarias para aplicar el poder global estratégico a varias situaciones de crisis en el mundo. Las capacidades de transporte aéreo son vitales para poder entregar fuerzas expedicionarias e infraestructura con un mínimo de demora.²¹ Estos recursos unen a los teatros y los lugares dentro del mismo teatro. El reaprovisionamiento de combustible amplía el alcance de las opciones de empleo disponibles para el comandante de la fuerza conjunta. Les permite a las aeronaves de combate, bombardero, de carga y de ala rotativa a operar desde bases que están seguras de ser atacadas y llevar a cabo misiones múltiples sin tener que regresar a la base cuando están bajas de combustible. El transporte espacial despliega sistemas espaciales para establecer capacidad operacional, sostener constelaciones de satélites fallidos o reemplazar satélites defectuosos y aumentar las constelaciones para incrementar la capacidad cuando la demanda de las operaciones globales actuales aumente.²²

Estas tres funciones se caracterizan por su capacidad para aumentar el alcance de los recursos militares y desplegar pertrechos a la contienda. Son una medida de nuestra aptitud para proyectar poder aéreo y espacial en el extranjero. Las operaciones dentro del ámbito ciberespacial logran el mismo efecto con la información como su carga útil. El *transporte cibernético* ocurre a menudo entre las computadoras conectadas vía la *Internet* u otras infraestructuras en la red. Es decir, paquetes de datos pasan por cables *Ethernet* y conexiones inalámbricas como mensajes comunicados entre los usuarios. Los administradores de redes que con frecuencia empujan paquetes y actualizaciones de *software* están llevando a cabo operaciones de transporte cibernético. Las imágenes y la información de inteligencia se comunican globalmente. Al igual que el transporte aéreo, el reaprovisionamiento de combustible en vuelo y el transporte espacial son los recursos físicos de nuestras fuerzas, las operaciones ciberespaciales son las facilitadoras de información. El transporte cibernético permite la entrega de información con precisión. Hacerle llegar la información correcta a la persona correcto en el momento correcto

es crítico en el entorno operacional de hoy, ya sea para llevar a cabo localización de blancos en los que el factor tiempo es decisivo o lanzando plataformas de carga en lugares “fuera del teatro”. La logística detrás del flujo de información enfocado representa un reto al que podemos responder usando las tácticas, técnicas y procedimientos correctos de transporte ciberespacial.

Inteligencia, Vigilancia y Reconocimiento

La información recopilada por los recursos de Inteligencia, Vigilancia y Reconocimiento (ISR), tales como el U-2 *Dragonlady*, satélites o personal secreto, contribuye a la creación de la preparación de inteligencia del espacio de la batalla (IPB), que provee información a los comandantes para ayudarles a entender y conocer al enemigo.²³ La manera más fácil, y quizás la que más se pasa por alto, de llevar a cabo ISR cibernético es sencillamente utilizar los buscadores de *Internet*. Las prácticas de las operaciones de seguridad para salvaguardar información esencial a menudo se pasan por alto o se implementan a la ligera, dándonos una oportunidad para recopilar fácilmente la inteligencia requerida. La enumeración de la red, otra actividad del ISR cibernético, incluye escanear las redes del adversario en busca de vulnerabilidades en su arquitectura de seguridad, permitiéndonos crear planes para explotar esas redes durante tiempo de guerra. Además, establecer señuelos dentro de nuestras propias redes les otorga a las fuerzas cibernéticas de Estados Unidos un lugar para aprender el tipo de información que nuestros enemigos buscan y las técnicas que ellos emplean para socavar nuestros protocolos de seguridad. Al utilizar *packet sniffers*, podemos apoderarnos y analizar paquetes que viajan en nuestras redes. Todas estas actividades nos permiten caracterizar las capacidades del enemigo con nuestros medios cibernéticos, proporcionando información adicional al IPB. Una vez dentro de las redes de nuestros adversarios, podemos aprovechar las operaciones cibernéticas ISR para llevar a cabo el IPB.

Operaciones Especiales

Las operaciones especiales utilizan las operaciones de poderío aéreo para llevar a cabo acciones que incluyen, pero no se limitan a, guerra no convencional, reconocimiento especial, PSYOP (operaciones psicológicas) y contra-terrorismo.²⁴ La diferencias entre las operaciones especiales y las operaciones convencionales radica en el grado de riesgo físico y político, manifestación, técnicas operacionales, modo de empleo, independencia de apoyo amigo y dependencia en operaciones de inteligencia detalladas y recursos autóctonos.²⁵

La naturaleza intrínsecamente clandestina de las operaciones especiales se compara con la facilidad de llevar a cabo operaciones cibernéticas encubiertas. En el 2007, los ataques cibernéticos invadieron a Estonia. Los periódicos, la banca y las agencias gubernamentales fueron sometidos a un ataque de negación de servicio distribuido por casi un millón de computadoras esclavizadas por los terroristas cibernéticos. Los servidores, enrutadores e interruptores del país se vieron inundados con tráfico y, por ende, se tornaron prácticamente inservibles. Muchos dedos señalaron al gobierno ruso. Los ataques llovían de todas partes de mundo, pero los funcionarios de seguridad de computadoras alegan que los atacantes fueron identificados por sus direcciones en la red, muchas de ellas rusas, y por instituciones estatales rusas.²⁶ Sin embargo, un problema importante con los ataques a la red tiene que ver con determinar con precisión la fuente. Según destaca el Dr. Martin Libicki, “Uno no podrá efectuar atribuciones razonables a menos que el agresor prácticamente anuncie su función”.²⁷ Por lo tanto, uno no puede responder sin atribuir razonablemente los ataques. Aún así, los ataques pueden venir de aliados o de nuestros propios sistemas.²⁸ Esto es bastante prometedor para aquellos que pueden aprovecharse de las vulnerabilidades del enemigo sin dejar un rastro cibernético.

Apoyo de Combate, Mando y Control, Búsqueda y Salvamento de Combate, Navegación y Posicionamiento y Servicios Meteorológicos

El apoyo de combate, mando y control (C2), búsqueda y salvamento de combate (CSAR), navegación y posicionamiento y los servicios meteorológicos son la columna vertebral de las funciones aéreas y espaciales mencionadas anteriormente. Sin el éxito de esas funciones, otras funciones no tienen, ni tendrán, éxito. El apoyo de combate es el resultado de operaciones exitosas de logística, médicas y de apoyo a la fuerza, cuya sinergia con otras operaciones es esencial para crear capacidad de combate a lo largo de la gama de esfuerzos militares.²⁹ El C2 incluye motivar a las fuerzas para que actúen con el fin de llevar a cabo la misión (mando) y regular esas mismas fuerzas para realizar operaciones acordes con la intención del comandante (control).³⁰ Un C2 eficaz le permite al comandante de la fuerza conjunta utilizar las plataformas disponibles de la Fuerza Aérea en el lugar y momento correctos, a pesar del fragor de la guerra, y degradar la capacidad de interceder del enemigo.³¹ CSAR es el método que la Fuerza Aérea emplea para apoyar la recuperación del personal conjunto en “entornos inciertos, negados u hostiles”.³² Las operaciones de recuperación de personal son esenciales para sostener el estado de ánimo de la unidad, conservar los recursos de combate esenciales y evitar que el enemigo consiga información de inteligencia.³³ Al proveer el lugar y tiempo de referencia precisos, la misión de navegación y posicionamiento le permite a las fuerzas militares maniobrar con precisión, sincronizar sus acciones, localizar y atacar blancos y ubicar y recuperar pilotos derribados. Los servicios meteorológicos ofrecen información oportuna y precisa sobre el espacio y los entornos atmosféricos. Esta información es esencial para coordinar, planificar y llevar a cabo operaciones aéreas y espaciales, por ende influenciando “la

selección de blancos, rutas, sistemas de armamento y tácticas de bombardeo”.³⁴

Las operaciones ciberespaciales permiten estas funciones, y la comunicación sobre el ámbito ciberespacial las facilita. En su mayoría, la navegación precisa y la coordinación dependen del ámbito ciberespacial para la transmisión de señales y la diseminación de datos de GPS. Las operaciones centradas en la red han dado paso para al apoyo continuo y eficaz de los guerreros, desde las necesidades básicas para administrar la tropa hasta los elementos de C2 requeridos. El sistema de armamento representado por el centro de operaciones aéreas y espaciales de la Fuera Aérea consiste en cientos de servidores ejecutando sistemas de informática, cada uno funcionando en el ciberespacio.

Contraciberespacial

Proponemos la siguiente definición para *contraciberespacial*: *Una función que consta de operaciones para lograr y mantener un grado deseado de superioridad ciberespacial mediante la destrucción, degradación o interrupción de las capacidades de un enemigo de usar el ciberespacio*. Esta definición es similar a las de otras funciones contra dominio que se mencionaron anteriormente. Aunque sí incluye el requisito de superioridad dentro del ámbito, esto difiere considerablemente de la opinión que tenemos de la superioridad aérea o espacial. En la versión borrador del AFDD 2-11 se define la superioridad ciberespacial como “el grado de ventaja que posee una fuerza sobre otra que le permite llevar a cabo operaciones en el ciberespacio en un momento y lugar determinado sin la interferencia prohibitiva de la fuerza opositora”.³⁵ La superioridad aérea y espacial se caracteriza por la libertad de acción y la libertad simultánea de ser atacado. La libertad de acción es una característica de la superioridad ciberespacial; sin embargo, debido a la naturaleza omnipresente de la Internet, la libertad de ser atacado no se puede garantizar y, por ende, no es un requisito para la superioridad ciberespacial. Un resumen adecuado de la superioridad ciberespacial sería “libertad de acción mediante el ataque” (o sea,

la capacidad de actuar aún bajo el ataque y después de un ataque). El General Kevin P. Chilton, Comandante del Comando Estratégico de Estados Unidos, concluyó que “salimos con nuestro atuendo de protección anti-NBQ para cumplir la misión (MOPP) y arreglamos aeronaves, las cargamos y las volamos. Llevamos a cabo operaciones en un entorno hostil. Así es como será operar bajo ataque en el ciberespacio”.³⁶ Podemos tener la certeza que el ciberespacio continuará siendo un entorno en disputa, pero esto no debe limitar nuestra capacidad para operar dentro del ámbito.

Como función, el contraciberespacio consta de varias operaciones relacionadas y no relacionadas con la cibernética. Por ejemplo, si el efecto deseado es interrumpir el servicio de *Internet*, entonces el ataque físico y la destrucción de equipo relacionada con la cibernética (por ejemplo, enrutadores y edificios que alojan a proveedores de servicio de *Internet*) se pueden considerar operaciones en apoyo al contraciberespacio. El efecto también podría ser en la forma de explotar un *software* para evitar que tráfico legítimo en la *Internet* fluya adecuadamente. Considere un ejemplo no clasificado. En mayo de 2007, el Presidente George W. Bush le ordenó a la Agencia de Seguridad Nacional que llevase a cabo un ataque cibernético contra teléfonos celulares y redes de computadora que los insurgentes iraquíes emplearon para planificar los bombardeos en las carreteras.³⁷ Las iniciativas de la agencia ayudaron a las fuerzas estadounidenses a incautar el sistema de comunicación de los insurgentes iraquíes. Antiguos funcionarios de la administración Bush involucrados con la decisión de ejecutar el ataque “acreditan a los ataques cibernéticos con permitirles a los planificadores militares poder rastrear y neutralizar algunos de los insurgentes más influyentes”, finalmente ayudando a cambiar el curso de la guerra.³⁸

Tanto las operaciones físicas como cibernéticas pueden surtir el mismo efecto en apoyo de la misión contraciberespacial, pero tienen distintos niveles de efectos indirectos que se deben tomar en cuenta. Por una parte, al igual que cualquier otro ataque, los ataques contra estructuras que alojan recursos cibernéticos

tienen el potencial de resultar en daños colaterales. Por otra parte, los ataques a través del ciberespacio contra recursos cibernéticos también pueden resultar en daños colaterales en cascada. El temor de tales efectos secundarios ha mantenido a los líderes estadounidenses alejados de apretar el gatillo del armamento cibernético. Antes de la reciente invasión a Irak por parte de Estados Unidos, se consideró un plan para inutilizar la red bancaria iraquí que luego se descartó cuando líderes del DoD determinaron que también socavaría a la banca francesa que está tan ligada a las instituciones iraquíes y podría posiblemente emigrar a los otros aliados, inclusive a Estados Unidos.³⁹

Tenemos que pensar seriamente al emplear una “munición” cibernética porque por lo regular no se destruye durante un ataque. Una vez lanzada, esa arma es fácil de capturar. Entonces, fuerzas cibernéticas pueden deconstruir y analizar su código para definir las contramedidas adecuadas para ataques futuros y para usarlas como un arma contra quien las envía.⁴⁰ Para lograr la superioridad ciberespacial, debemos llevar a cabo operaciones exitosas de ofensiva, defensiva y de mantenimiento mediante el ataque a la red, defensa de la red y operaciones en la red, respectivamente, para poder lograr el nivel de control necesario para operar sin impedimentos a la vez que evitamos que el enemigo le saque ventaja al uso del ciberespacio.⁴¹ Elevar las operaciones contraciberespaciales como una misión de la Fuerza Aérea ayudará a dar un enfoque y establecer fronteras para el servicio y la comunidad conjunta.

Conclusión

Toda doctrina operacional ciberespacial debe tomar en cuenta las similitudes entre y las relaciones con las operaciones aéreas y espaciales. Muchas personas están de acuerdo con el borrador del enunciado de la doctrina de las operaciones ciberespaciales que el ámbito ciberespacial es un ámbito virtual *hecho por el hombre*. Estudios adicionales revelan sus similitudes *naturales* con otros ámbitos, según lo define el entorno del espectro electromag-

nético. Si se mira el ámbito ciberespacial como la quinta dimensión (del aire, tierra, mar y espacio), más personas concluirán que no es diferente a las otras cuatro dimensiones, donde creamos y utilizamos tecnología hecha por el hombre para entrar, maniobrar y explotar esos ámbitos.⁴² Además, las características singulares del ámbito ciberespacial dictan cómo operamos dentro de él.

El *ciberespacio* es una expresión capciosa que invoca varias definiciones de diferentes organizaciones y personas.⁴³ Ya que cuenta con experiencias operacionales limitadas en el ciberespacio, la Fuerza Aérea debe emplear su experiencia en otros ámbitos bélicos para poder elaborar una doctrina acertada. Después de todo, las operaciones ciberespaciales apoyan las mismas funciones que las operaciones aéreas y espaciales. Tal como escribiera Michael W. Wynne, Secretario de la Fuerza Aérea, “Todos los aspectos de la guerra aérea desempeñarán algún papel equivalente en la guerra cibernética”.⁴⁴ Con el advenimiento de las operaciones ciberespaciales, algunos cambios tiene que suceder, que incluyan diferenciar las operaciones ciberespaciales de las IO. Además, se debe agregar una nueva función contraciberespacial para recalcar su importancia como una función independiente de la Fuerza Aérea en el ámbito ciberespacial. Tal como Londsedale destaca, “Aunque el ciberespacio tiene un papel que desempeñar en todas las dimensiones, fundamentalmente no cambia nada con verdadero significado en la estrategia. Por lo tanto, al igual que la dimensión aérea antes del mismo, el ciberespacio afecta la gramática de la guerra pero no su lógica”.⁴⁵

Con el tiempo, nuestra experiencia en llevar a cabo operaciones ciberespaciales y trabajar en el ámbito ciberespacial aumentará y se arraigará a nuestras operaciones diarias; aceptaremos esas operaciones de la misma manera que aceptamos las operaciones aéreas y espaciales. La doctrina ciberespacial evolucionará de manera que podamos materializar las ideas en práctica de la manera más eficaz posible. Mientras, debemos analizar y aprender de las similitudes y diferencias entre las operaciones aéreas, espaciales y ciberespaciales en apoyo a las misiones aérea, espacial y ciberespacial. □

Notas

1. “Los observadores constantemente describen la guerra de su propia era como una que marca una brecha revolucionaria en el progreso normal de los métodos de la guerra. Su selección de su propia era debe poner en aviso a los lectores y oyentes.... Es una falacia, a causa de la falta de conocimientos de la historia militar técnica y táctica, suponer que los métodos de la guerra no han hecho un progreso continuo y, en general, bastante constante”. Cyril B. Falls, *A Hundred Years of War* (Cien años de Guerra) (London: Duckworth, [1953]), 13.
2. Honorable Michael W. Wynne, “Flying and Fighting in Cyberspace,” (Volar y luchar en el ciberespacio) *Air and Space Power Journal*, (Tercer Trimestre 2007): 3, <http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf> (accessed 8 December 2009).
3. Air Force Doctrine Document 1, *Air Force Basic Doctrine* (Documento 1 de Doctrina de la Fuerza Aérea, Doctrina Básica de la Fuerza Aérea), 17 de noviembre de 2003, 3, http://www.dtic.mil/doctrine/jel/service_pubs/afdd1.pdf (consultado el 8 de diciembre de 2009).
4. Dr. David J. Lonsdale, “The Impact of Cyberspace on Strategy,” (El impacto del ciberespacio en la estrategia) *High Frontier* 5, no. 3 (May 2009): 23, <http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf> (consultado el 8 de diciembre de 2009).
5. AFDD 1, *Air Force Basic Doctrine*, 39.
6. *Ibid.*, 39-40.
7. AFDD 2-1.2, *Strategic Attack* (Ataque estratégico), 12 June 2007, 2, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_2.pdf (consultado el 8 de diciembre de 2009).
8. Col John A. Warden, *The Air Campaign: Planning for Combat* (La campaña aérea: Planificando para el combate) (Washington, DC: National Defense University Press, 1988), <http://www.au.af.mil/au/awc/awcgate/warden/warden-all.htm> (consultado el 8 de diciembre de 2009).
9. Dr. Dan Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” (Del ciberespacio al ciberpoder: Definiendo el problema) en *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 6.
10. Kim Zetter, “Simulated Cyberattack Shows Hackers Blasting Away at the Power Grid,” (Ataque cibernético simulado muestra a los hackers atacando las subestaciones de potencia) 26 September 2007, *Wired*, <http://www.wired.com/threatlevel/2007/09/simulated-cyber/> (consultado el 8 de diciembre de 2009).
11. Brian Krebs, “Report: Russian Hacker Forums Fueled Georgia Cyber Attacks,” (Informe: Foro ruso de hackers avivó ataques cibernéticos en Georgia) *Washington Post*, 16 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (accessed 8 December 2009).
12. AFDD 1, *Air Force Basic Doctrine*, 41.
13. AFDD 2-1.1, *Counterair Operations* (Operaciones contraaéreas), 1 October 2008, 5, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_1.pdf (consultado el 8 de diciembre de 2009).
14. AFDD 2-2.1, *Counterair Operations* (Operaciones contraaéreas), 2 August 2004, 3, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_1.pdf (consultado el 8 de diciembre de 2009).
15. AFDD 1, *Air Force Basic Doctrine*, 43.
16. Department of Defense, *Quadrennial Roles and Missions Review Report* (Informe trimestral de la revisión de las funciones y misiones) (Washington, DC: Department of Defense, January 2009), 16, <http://purl.access.gpo.gov/GPO/LPS108437> (consultado el 8 de diciembre de 2009).
17. Associated Press, “Hacker Forces 1,500 Pentagon Computers Offline” (Hacker saca fuera de línea a 1,500 computadoras en el Pentágono), 21 June 2007, <http://www.msnbc.msn.com/id/19358920/> (consultado el 15 de agosto de 2009).
18. En la Publicación Conjunta 3-13, Operaciones de Información, del 13 de febrero de 2006, y en la Directriz 3600.01 del DOD, Operaciones de Información, del 14 de agosto de 2006, se mencionan más específicamente a la guerra electrónica, las operaciones en la red de computadoras, operaciones psicológicas, engaño militar y operaciones de seguridad como las cinco aptitudes básicas de las IO.
19. “Sencillamente, la guerra electrónica (EW) no forma parte del ciberespacio. La cibernética es cliente de la EW. Sí emplea aspectos limitados de la EW, pero ésta sirve otros cuatro ámbitos—tierra, mar, aire y espacio—que también necesitan lograr control del espectro. Dentro del Servicio Conjunto, la opinión predominante indicaría que la EW de hecho permanecerá como un área de misión articulada para ejercer el cuidado y la protección esencial del espectro, y no para ser asimilada por ninguna área de misión semejante, tal como la cibernética”. Lt Col Jesse Bourque, “Does EW + CNO = Cyber?” (¿Acaso EW + CNO – Cibernética? *Journal of Electronic Defense* 31, no. 9 (September 2008): 34.
20. AFDD 2-5, *Information Operations* (Operaciones de información), 11 January 2005, 23, <http://www.carlisle.army.mil/DIME/documents/afdd2-5InformationOperations.pdf> (consultado el 8 de diciembre de 2009).
21. AFDD 2-1, *Air Warfare* (Guerra aérea), 22 January 2000, 17, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1.pdf (consultado el 8 de diciembre de 2009).
22. *Ibid.*, 18-19.
23. *Ibid.*, 20-21.
24. AFDD 1, *Air Force Basic Doctrine*, 53. El término PSYOP (operaciones psicológicas) ha sido cambiado a MISO (Military Information Support Operation)
25. AFDD 2-7, *Special Operations* (Operaciones especiales), 16 December 2005, 3, <http://www.fas.org/irp/doddir/usaf/afdd2-7.pdf> (consultado el 8 de diciembre de 2009).
26. Ian Traynor, “Russia Accused of Unleashing Cyberwar to Disable Estonia,” (Rusia es acusada de desencadenar una guerra cibernética para neutralizar a Estonia) *Guardian*, 17 May 2007, <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> (consultado el 1º de julio de 2009).

27. Dr. Martin Libicki, "Deterrence in Cyberspace," (La disuasión en el ciberespacio) *High Frontier* 5, no. 3 (May 2009): 18, <http://www.afspc.af.mil/shared/media/document/AFDD-090519-102.pdf> (consultado el 8 de diciembre de 2009).

28. Shane Harris, "The Cyberwar Plan," (El plan para la guerra cibernética) *National Journal Magazine*, 14 November 2009, http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (consultado el 14 de noviembre de 2009).

29. AFDD 1, *Air Force Basic Doctrine*, 47.

30. AFDD 2-1, *Air Warfare*, 14-15.

31. AFDD 2-8, *Command and Control*, (Mando y control) 1 June 2007, 4-6, <http://www.fas.org/irp/doddir/usaf/afdd2-8.pdf> (consultado el 8 de diciembre de 2009).

32. AFDD 2-1.6, *Personnel Recovery Operations*, (Operaciones de recuperación de personal), 1 June 2005, 10, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD2-1.6.pdf> (consultado el 15 de diciembre de 2009).

33. AFDD 1, *Air Force Basic Doctrine*, 57.

34. AFDD 2-1, *Air Warfare*, 24-15.

35. AFDD 2-11, "*Cyberspace Operations*," (Operaciones ciberespaciales) borrador, 4 de febrero de 2008, 13.

36. Gen Kevin P. Chilton, "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," (Liderazgo ciberespacial: Hacia una nueva cultura, conducta y aptitudes) *Air and Space Power Journal* 23, no. 3 (Fall 2009):

10, <http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf> (consultado el 8 de diciembre de 2009).

37. Harris, "Cyberwar Plan."

38. Ibid.

39. Ibid.

40. Ibid.

41. AFDD 2-11, "*Cyberspace Operations*," (Operaciones ciberespaciales) borrador, 13-17.

42. Kuehl, "From Cyberspace to Cyberpower," (Del ciberespacio al ciberpoder), 4.

43. En un memorando del Secretario Adjunto de Defensa, con fecha del 12 de mayo de 2008, el DOD define el *ciberespacio* "como un ámbito global dentro del entorno de información que consta de la *red interdependiente de infraestructuras de la tecnología de información, incluyendo la Internet, redes de telecomunicaciones, sistemas de computadora y procesadores y controladores incorporados*. Las doctrina de la Fuerza Aérea lo define como "un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos vía sistemas en la red e infraestructuras físicas afines". AFDD 2-11, "*Cyberspace Operations*," (Operaciones ciberespaciales) borrador, 1.

44. Wynne, "Flying and Fighting in Cyberspace," 8.

45. Lonsdale, "Impact of Cyberspace on Strategy," 21.



El **Mayor Eric D. Trias** (BS, University of California-Davis; MS, Air Force Institute of Technology [AFIT]; PhD, University of New Mexico) es profesor adjunto de ciencias computacionales en la Facultad de Ingeniería Eléctrica y de Computadoras en el Instituto de Tecnología de la Fuerza Aérea (AFIT), Base Aérea Wright-Patterson, Ohio. En 1988, el Mayor Trias ingresó a la Fuerza Aérea y en 1994 fue otorgado el premio de Doce Hombres del Aire Excelentes del Año. En 1998 recibió su comisión a través del Programa de Educación y Nombramientos y de la Escuela de Capacitación para Oficiales. En calidad de oficial de comunicaciones, el Mayor Trias ha servido en la Base Aérea Osan y en el Campamento Humphreys del Ejército, República de Corea, y en el Centro de Operaciones de Misiones Distribuida en la Base Aérea Kirtland, New Mexico. Es egresado de la Escuela para Oficiales de Escuadrón y de la Escuela Superior de Comando y Estado Mayor. Entre las investigaciones actuales del Mayor Trias se encuentran descubrimiento de conocimientos y minería de datos, seguridad en los sistemas de informática, ciencias forenses digitales y varios temas relacionados con el ciberespacio.



El **Capitán Bryan M. Bell** (BS, University of Florida) está cursando estudios para obtener una Maestría en Ciencias, con especialización en ciencias espaciales, en la Facultad de Aeronáutica y Astronáutica en el Instituto de Tecnología de la Fuerza Aérea (AFIT), Base Aérea Wright-Patterson, Ohio. En el 2005 recibió su comisión a través del Cuerpo de Capacitación para Oficiales de la Reserva y se dedicó a la carrera de operaciones espaciales y de misiles. Antes de asistir a AFIT, se desempeñó en calidad de comandante de tripulación e instructor en advertencia de misiles, 7o Escuadrón de Advertencia Espacial, Base Aérea Beale, California. Al egresar de AFIT, el Capitán Bell se desempeñará como oficial a cargo de los planes del componente, Centro de Inteligencia Conjunta del Comando Estratégico de EE.UU., Fuerte Meade, Maryland.

Declaración de responsabilidad: Las ideas y opiniones expresadas en este artículo reflejan la opinión exclusiva del autor elaboradas y basadas en el ambiente académico de libertad de expresión de la Universidad del Aire. Por ningún motivo reflejan la posición oficial del Gobierno de los Estados Unidos de América o sus dependencias, el Departamento de Defensa, la Fuerza Aérea de los Estados Unidos o la Universidad del Aire. El contenido de este artículo ha sido revisado en cuanto a su seguridad y directriz y ha sido aprobado para la difusión pública según lo estipulado en la directiva AFI 35-101 de la Fuerza Aérea.