

# Reenfoque del Pensamiento de la Guerra Cibernética

MAYOR SEAN C. BUTLER, USAF



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

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

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

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

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

## El ciberespacio como dominio físico

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

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

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

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

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

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

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

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

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

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

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

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

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

## El carácter exclusivo del ciberespacio

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

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

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

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

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

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

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

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

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

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

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

## Conclusión

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

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

### Notas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. *Ibid.*, 5.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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