

# 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.<sup>1</sup>

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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup> 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”.<sup>5</sup> 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”.<sup>6</sup> 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”.<sup>7</sup>

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).<sup>8</sup> 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”.<sup>9</sup>

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”.<sup>10</sup> 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).<sup>11</sup> 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).<sup>12</sup>

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”.<sup>13</sup> 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).<sup>14</sup> 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”.<sup>15</sup> 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”.<sup>16</sup> 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*.<sup>17</sup> (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.”<sup>18</sup> 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”.<sup>19</sup> 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”.<sup>20</sup> 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]”.<sup>21</sup> 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”.<sup>22</sup>

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.<sup>23</sup> 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.<sup>24</sup> 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.<sup>25</sup> 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.<sup>26</sup> 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).<sup>27</sup>

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](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](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](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](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](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/](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](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](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.