Preparándonos para el campo de batalla cibernético del futuro

Subteniente (2nd Lt) Christopher Babcock, USAF

Para los hombres del aire dedicados a los ámbitos espacial y cibernético, la contienda del mañana será definida en gran medida por el concepto de la dependencia ciberespacial. Ese término, según lo define el autor, es el grado al cual la capacidad militar depende de la supremacía sobre una porción del ámbito ciberespacial para poder ocasionar o llevar a cabo sus efectos.[1] La dependencia en la cibernética está creciendo rápidamente a causa de la naturaleza exponencial del ámbito ciberespacial, la trayectoria de las fuerzas del mercado en el mundo civil y la integración estratégica de la tecnología de las computadoras por parte de los militares en los ámbitos terrestre, marítimo y aéreo.[2]

A diferencia del empleo en los tres ámbitos bélicos tradicionales, el empleo actual de las capacidades en el ámbito del espacio *no se puede alcanzar* sin el espacio cibernético.[3] El reconocimiento de esta relación singular entre el espacio y el espacio cibernético tiene implicaciones profundas, para el reclutamiento; la formación inicial, intermedia y avanzada y el desarrollo en los campos profesionales espacial y cibernético. Una transición del sistema actual de la formación de la fuerza hacia uno que reconozca que la relación singular entre el espacio y el espacio cibernético tendrá el beneficio adicional de informar a la comunidad operacional en general a medida que los guerreros en los ámbitos terrestre, marítimo y aéreo continúan dependiendo cada vez más del espacio cibernético y del espacio. En este artículo se tratan las implicaciones de la dependencia en la cibernética y se proponen seis recomendaciones para garantizar que desde el reclutamiento hasta el adiestramiento avanzado, los hombres del aire dedicados al espacio y a la cibernética estén preparados para sobresalir en sus ámbitos interconectados.

Dependencia del espacio en la cibernética

> *La relación entre el espacio y el espacio cibernético es singular porque prácticamente todas las operaciones espaciales dependen del espacio cibernético y una porción crítica de éste solamente se puede proporcionar a través de las operaciones espaciales.*
>
> —Publicación Conjunta 3-12 (R),
> *Operaciones Ciberespaciales, 5 de febrero de 2013*

Todas las operaciones espaciales que la milicia estadounidense lleva a cabo en la actualidad dependen del espacio cibernético (fig. 1).[4] Las operaciones espaciales tienen lugar en el ámbito espacial físico, no dentro del espacio cibernético. Pero en vista de que aquellos que llevan a cabo las operaciones espaciales no están presentes físicamente en el espacio, deben depender completamente en el control de su segmento del espacio cibernético para transmitir sus comandos a los vehículos espaciales para poder llevar a cabo las operaciones espaciales.[5]

Si una operación espacial militar involucrase a un piloto que reside físicamente en un vehículo espacial, reaccionando al entorno para poder llevar a cabo efectos en el espacio, esto describiría una operación espacial que no depende en su totalidad de la supremacía del espacio cibernético.[6] A falta de ese escenario, los operadores espaciales deben emplear computadoras y programas de computadoras especializados para transmitir información desde y hacia sus vehí-

culos espaciales —que en sí son sistemas de informática complejos— a través de una red de computadoras.[7] La dependencia del espacio en la cibernética exige que se preste atención especial a la defensa cibernética de las capacidades espaciales, pero también presagia el estado futuro de los ámbitos bélicos tradicionales.

La capa de la red física del espacio cibernético incluye los sistemas de informática con los cuales los operadores espaciales controlan sus satélites, los circuitos conectando esos sistemas de informática al equipo terrestre y el equipo terrestre en sí. La capa de la red lógica del espacio cibernético está integrada en cada pedazo de la red física. La capa de personas especializadas en cibernética describe a los operadores espaciales que dependen de las capas física y lógica de la red para llevar a cabo las operaciones espaciales (fig. 2).

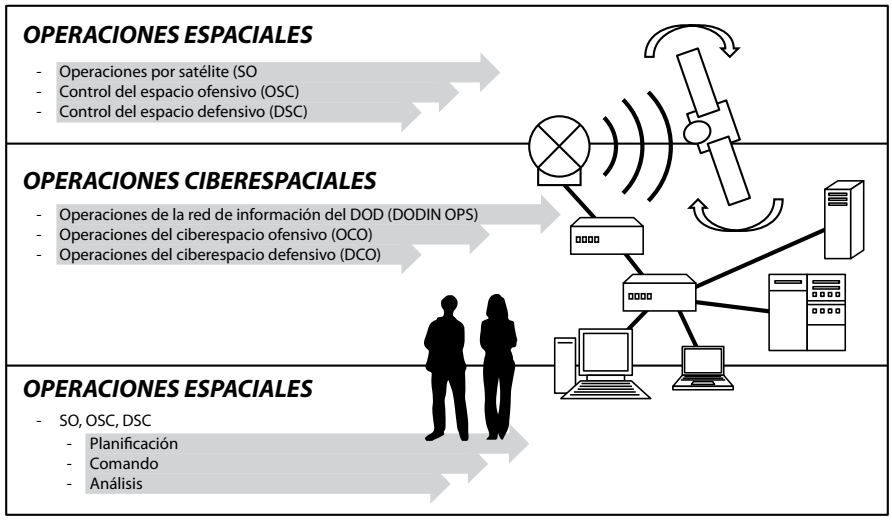

Figura 1. Operaciones espaciales y ciberespaciales. A causa de las limitaciones físicas, las operaciones espaciales tienen lugar en ambos lados del ámbito ciberespacial.

El ámbito exponencial

Pero si usted piensa que está seguro en la cibernética, mañana cuando despierte, todo será diferente.

—Gen John E. Hyten, Comandante
Comando Espacial de la Fuerza Aérea

Desde que el cofundador de la inteligencia, el Sr. Gordon Moore, destacó en 1965 que la capacidad de los circuitos de las computadoras crece exponencialmente con el tiempo, se ha admitido generalmente que la innovación en la tecnología de las computadoras crece a una velocidad incomparable en la historia de la humanidad.[8] La innovación engendra innovación, y la naturaleza evolutiva de la tecnología de la informática plantea retos singulares para los operadores militares en el ámbito ciberespacial en comparación con aquellos de los primeros cuatro ámbitos bélicos.[9]

El primero entre esos retos se encuentra el hecho de que el sector privado ahora ha comenzado a avanzar mucho más rápido que la industria de la defensa en varios campos de la innovación tecnológica.[10] Esto se puede atribuir en su mayoría a los procesos de gestión de compra y configuración tipo extracción de melaza en los programas tecnológicos grandes del Departamento de Defensa con relación a la agilidad de una compañía emergente del *Silicon Valley* (Valle del Silicio).[11]

Un segundo reto grave es que la asimetría del espacio cibernético les permite a los agresores utilizar más rápida y fácilmente los cambios rápidos a su favor que lo que pueden los defensores.[12] A un nivel fundamental, los defensores cibernéticos intentan cerciorarse que el *software* y el *hardware* funcionen como deben mientras que los agresores cibernéticos intentan interrumpir el *software* o *hardware* para ocasionar efectos nocivos.[13] En este ajuste, el agresor casi siempre tiene la ventaja. Además, la naturaleza exponencial del espacio cibernético ocasiona que el conocimiento institucional y los conjuntos de destrezas individuales se atrofien mucho más rápido que en los ámbitos bélicos tradicionales. Esto plantea retos especialmente interesantes para el adiestramiento y educación de los operadores ciberespaciales.

A pesar de todas sus dificultades, la Fuerza Aérea de Estados Unidos tiene un entendimiento bien establecido sobre el campo de batalla cibernético actual. Sin embargo, debe dar cuenta completamente por la naturaleza de la dependencia cibernética y las repercusiones que tiene para el campo de batalla cibernético del futuro.

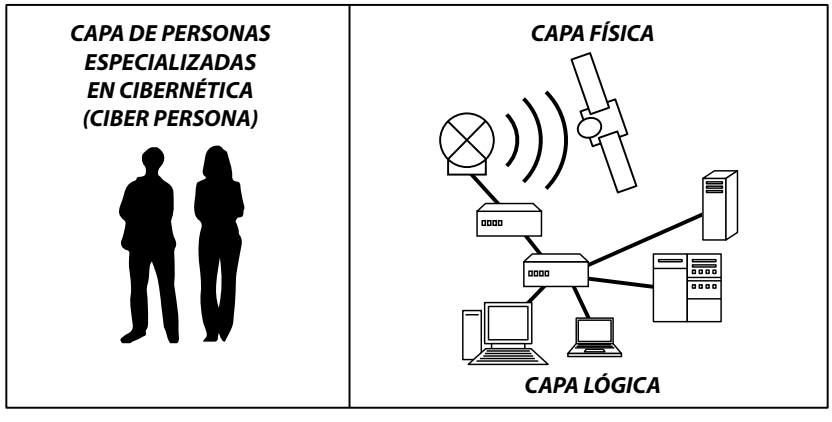

Figura 2. Capas cibernéticas en las operaciones espaciales

Dependencia autoinducida

El F-35 Lightning II es uno de los sistemas de armamento más complicados que jamás se haya diseñado, un avión a reacción de combate y furtivo que tomó años en fabricar y que a menudo se le conoce como una computadora voladora por sus más de ocho millones de líneas de códigos.

—Christian Davenport, Washington Post

Si bien el ámbito espacial es el primero en depender completamente de la cibernética, no continuará siendo el único. En el ámbito aéreo, las aeronaves piloteadas por control remoto son un ejemplo excelente de un sistema de armamento que depende completamente de la ciberné-

tica.[14] Inclusive, el avión de combate más nuevo, el F-35, se ha descrito como una computadora voladora; además, mientras que el Ejército diseña aeronaves teledirigidas personales, dermatoesqueletos inteligentes y rifles computarizados, la Agencia de Proyectos de Investigación Avanzados de la Defensa está diseñando robots con mochilas y la Armada está diseñando sus propias aeronaves teledirigidas autónomas, inclusive submarinos y aeronaves.[15]

Si bien esas iniciativas, de hecho, mejorarán las capacidades bélicas, una mayor dependencia en la cibernética viene con un precio. El coste se pude sufragar en mayor riesgo a las misiones que esas tecnologías apoyan o en seguridad deliberada y defensa activa de los sistemas recién dependientes.[16] En cada ejemplo, los riesgos intrínsecos introducidos por la dependencia en la cibernética son monumentales. En el mundo civil, los piratas informáticos ya han podido controlar esos vehículos (más notablemente logrando el control remoto completo de los últimos modelos de *Jeep*), pistolas inteligentes y aviones teledirigidos de pasatiempo. Inclusive, han infiltrado las redes internas de aeronaves comerciales.[17] Para el escuadrón cibernético del futuro, la seguridad y la defensa de los sistemas de armamento locales —desde tierra y aire hasta el espacio— deben ser una prioridad (fig. 3).

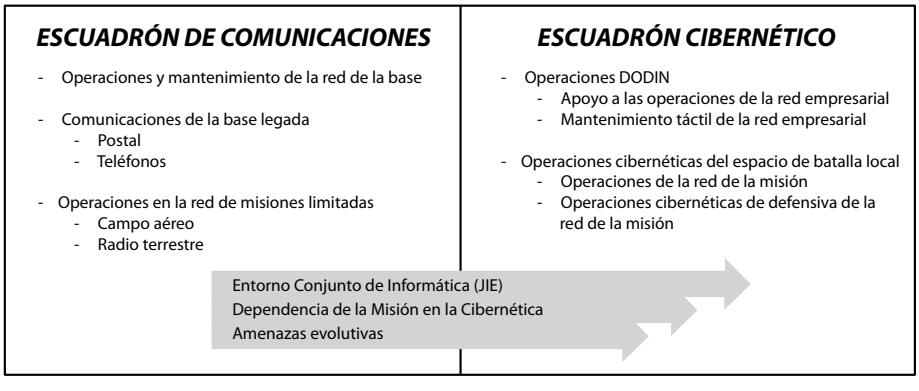

Figura 3. De las comunicaciones a la cibernética. (Basado en parte en resumen informativo, Tte Cnel David Canady, Asunto: Escuadrón cibernético del futuro, Cuartel General de la Fuerza Aérea / A6CF, mayo de 2014, http://www.safcioa6.af.mil/shared/media/document/AFD-140512-040.pdf.)

Un reto particularmente escabroso para aquellos operadores cibernéticos será el requisito de llevar a cabo operaciones cibernéticas en la red viva de un sistema de armamento, pero este reto se puede y se debe vencer.[18] Optar por no asegurar ni defender es la opción más arriesgada de todas. En el espacio cibernético, mientras más tiempo haya una vulnerabilidad en una forma no mitigada, mayores son las probabilidades que será convertida en una forma destructiva y explotada por un adversario. En algunos aspectos el proceso, desde el descubrimiento hasta la forma destructiva y el ataque, a los piratas cibernéticos les toma poco más de una semana para completarlo.[19]

Las inquietudes sobre la seguridad cibernética aún no han detenido al Departamento de Defensa de obtener armamento que depende cada vez más de la cibernética. En el mundo civil, los consumidores habituales también parece que aún no son convencidos por las inquietudes de seguridad.

Dependencia en la cibernética impulsada por el mercado

Estas características y condiciones presentan una paradoja dentro del espacio cibernético: la prosperidad y seguridad de nuestra nación han sido mejoradas significativamente por nuestro uso del espacio cibernético, sin embargo esos mismos progresos han conducido a mayores vulnerabilidades y una dependencia crítica en el espacio cibernético, para Estados Unidos en general y la fuerza conjunta en particular.

—Publicación Conjunta 3-12 (R),
Operaciones Ciberespaciales, 5 de febrero de 2013

Las fuerzas del mercado en el mundo civil están conduciendo rápidamente a muchas categorías de productos del consumidor hacia la *"Internet of Things"* (Internet de las cosas) (IoT, por sus siglas en inglés). Se calcula que para el año 2020 habrá entre 50 a 100 mil millones de dispositivos conectados entre sí en la red por todo el mundo, creando una IoT.[20]

Desde refrigeradoras hasta cafeteras y termostatos, el mercado comercial está siendo inundado cada vez más con *dispositivos de Internet* de todo tipo.[21] Se puede decir que la preponderancia de dispositivos en el mercado en el futuro cercano serán más sensibles a la Internet, dificultándole a un consumidor perspicaz como el Departamento de Defensa encontrar alternativas no computarizadas.[22] Esto deja a los militares con opciones difíciles de tomar con respecto a la compensación entre aceptar el riesgo o aceptar los costes relacionados con la seguridad cibernética y la defensa de esos refrigeradores y cafeteras recién incorporadas a la red.

Si aceptamos que en el futuro un porcentaje mucho mayor de dispositivos, infraestructuras y sistemas tendrán capacidades de redes informáticas que son o bien parte permanente de las instalaciones militares (tales como supervisión, control y adquisición de datos [SCADA]) o entrarán con regularidad a las instalaciones militares (tales como relojes inteligentes y vehículos sin conductor), entonces esos dispositivos se convertirán en una parte de *facto* del espacio de batalla cibernético. El escuadrón cibernético del futuro es en el que se debe depender para asegurar y defender esos dispositivos. Los rendimientos provistos por cambios orgánicos y estructurales tales como el cambio hacia el entorno conjunto de informática, al igual que las nuevas tecnologías tales como el establecimiento de redes definidas por *software*, puede que liberen muchos de los recursos requeridos para permitir que el escuadrón cibernético del futuro asegure y defienda el terreno cibernético más amplio; no obstante, inversiones y reformas adicionales también serán necesarias para apoyar esos requerimientos nuevos.[23]

Ganando la contienda del mañana

En vista del rápido avance hacia mayor dependencia en la cibernética en la milicia, es esencial que el Comando Espacial de la Fuerza Aérea examine y considere las siguientes recomendaciones para los sistemas de desarrollo de la fuerza cibernético y espacial.[24]

Sacarle provecho a los grandes datos para la toma de decisiones

El Comando Espacial de la Fuerza Aérea debe crear tres pruebas estandarizadas y debe implementarlas a lo largo del proceso de formación de la fuerza para evaluar a los hombres del aire dedicados al espacio y a la cibernética. La primera prueba debe ser solamente solamente para la pericia e inclinación a la cibernética. Esta prueba mediría el potencial de un recluta o estudiante para comprender los conceptos cibernéticos y adquirir destrezas cibernética, indistintamente del entrenamiento cibernético oficial.[25] La segunda y la tercera prueba serían basadas en el conocimiento —una para el conocimiento pertinente a las operaciones ciberespaciales y la otra per-

tinente al espacio. Inicialmente, puede que sea imposible determinar exactamente qué es la pericia cibernética. Esto es aceptable y no debe disuadir al comando de emprender ese esfuerzo. A medida que se recopilan las calificaciones de las tres pruebas, se deben asociar con los miembros y monitorearlas con otras medidas para determinar cómo tienen relación con el éxito, mediocridad y fracaso de un individuo en particular. El proceso de recopilación de datos y análisis informa de manera continua una reevaluación cíclica de las pruebas para garantizar que evalúen correctamente la capacidad y el conocimiento.

Los puntos pertinentes de los datos que se deben asociar con las calificaciones de las pruebas se incluyen en tres categorías principales: educación, adiestramiento y experiencia. Al combinar las calificaciones de las pruebas de pericia y conocimiento con los puntos de los datos de esas tres categorías, el Comando Espacial de la Fuerza Aérea obtendrá una información poderosa sobre cómo priorizar la educación, adiestramiento y experiencia al tomar decisiones relacionadas con la formación de la fuerza. Al reevaluar estratégicamente a los hombres del aire, el comando puede obtener información sobre cómo eventos de adiestramiento específicos o hitos afectan o no las calificaciones.[26]

Adiestramiento cibernético específico a la misión

El Comando Espacial de la Fuerza Aérea está a punto de implementar el marco óptimo para un sistema de adiestramiento inicial, intermedio y avanzado para las operaciones ciberespaciales. El enfoque actual en el entrenamiento intermedio específico a la misión en lugar del entrenamiento intermedio general y entrenamiento en el trabajo es un gran paso en la dirección correcta.[27] Mayores dependencias en la cibernética crearán la necesidad de cursos de adiestramiento adicionales específicos a la misión tales como SCADA y las operaciones defensivas IoT, al igual que entrenamiento defensivo cibernético intermedio que es específico a varios sistemas de misiones terrestres, espaciales y aéreas.

Para los suboficiales de la Fuerza Aérea, el curso de entrenamiento inicial del 1B debería dividirse entre una combinación de un curso de entrenamiento inicial del 3D y del 1B específicos para los requisitos de la misión que los suboficiales 1B y 3D enfrentarán. El campo profesional 3D no debe excluirse del funcionamiento de los campos profesionales de las comunicaciones porque desempeña papeles importantes en la seguridad y la defensa del campo de batalla cibernético y lo continuará haciendo. Los esfuerzos para dividir los requerimientos de entrenamiento entre los campos profesionales 3D y 1B deben seguir la Iniciativa Nacional del Marco de Educación para la Seguridad Cibernética del Instituto Nacional de Estándares y Tecnología.[28] Si bien el entrenamiento para los suboficiales en los campos profesionales 3D y 1B se desviará rápidamente después de los principios básicos, debe haber un conjunto de conceptos básicos de "cibernética operacional" compartidos por los dos campos profesionales.[29]

Capacitación especializada para los operadores que dependen de la cibernética

Para aquellos oficiales que no se especializan en la cibernética cuyos conjuntos de misiones contienen altos niveles de dependencia en la cibernética, tales como personal de operaciones espaciales y pilotos de aeronaves controladas por control remoto, se les deben ofrecer oportunidades para asistir al entrenamiento en cibernética intermedio y avanzado pertinente a su misión. La aceptación al programa para los hombres del aire especializados en cibernética se debe basar en su pericia en la cibernética y las calificaciones en las pruebas de conocimiento.

Al igual que hay una ventaja con poder contar con oficiales que son expertos a lo largo de los sistemas de armamento, también sería ventajoso poder contar con oficiales en misiones que dependen de la cibernética que también son expertos en las operaciones cibernéticas.[30] Un programa de muchas maneras similar al que ofrece la Escuela de Armamento de la USAF pero con un impacto más pequeño se debería establecer para colocar estratégicamente a los egresados dentro de sus campos profesionales que dependen de la cibernética.[31]

Trabajar para ampliar las oportunidades de asociaciones en la industria

El Comando Espacial de la Fuerza Aérea debe colaborar con la Oficina del Asistente al Secretario de la Fuerza Aérea para la Adquisición (SAF/AQ, por sus siglas en inglés) y con el Instituto de Tecnología de la Fuerza Aérea (AFIT, por sus siglas en inglés) para crear un programa especial para oficiales y suboficiales de la Fuerza Aérea en los campos profesionales espacial y cibernético para que participen en el programa Educación con la Industria (EWI, por sus siglas en inglés). Si esto no se puede lograr, el Comando Espacial de la Fuerza Aérea debe estudiar la posibilidad de establecer un programa similar, enfocado en traer de nuevo a la milicia innovación avanzada y destrezas especializadas a la vez que amplía sus lazos con los socios en la industria.

Los egresados del programa EWI no solo ayudan a cerrar la brecha de la tecnología y las destrezas entre la milicia y el sector privado sino que también aumentan la cooperación y fortalecen los lazos entre los dos sectores en un momento crítico para el espacio y el espacio cibernético.[32] El Comando Espacial de la Fuerza Aérea se debe enfocar en incorporar a oficiales y suboficiales de la Fuerza Aérea dentro de corporaciones que están a la vanguardia de la tecnología espacial y ciberespacial y debe intensificar su expansión fuera de la lista de contratistas tradicionales aprobados por la defensa.

Aunque el programa EWI por lo general no está disponible a los suboficiales, el espacio y el espacio cibernético requieren destrezas técnicas singulares que se pueden desarrollar y cultivar en un servicio EWI. Si bien un oficial en el programa EWI puede desarrollar destrezas de liderazgo singulares y aprender ideas innovadoras, un suboficial colocado correctamente podría fortalecer sus técnicas de codificación u otras que son específicas a su misión y campo profesional.

Estos esfuerzos estarían acordes con las iniciativas del Secretario de la Defensa, Ashton Carter, para aumentar la innovación en el Departamento de Defensa y fortalecer los lazos entre la milicia y la industria.[33] Además, en coordinación con SAF/AQ y AFIT en el programa EWI, el Comando Espacial de la Fuerza Aérea debería establecer lazos directos con la Unidad X de Innovación de la Defensa, la nueva célula del Departamento de Defensa en el Silicon Valley.[34] En vista de que la Unidad X principalmente desarrollará y fortalecerá lazos con la industria en el campo de las operaciones cibernéticas, el Comando Espacial de la Fuerza Aérea se beneficiaría de coordinar con la Unidad X en el desarrollo de la fuerza de los operadores ciberespaciales.[35]

Promover nuevas formas de educación y adiestramiento

El mercado civil para *microdegrees* (micro grados), *nanodegrees* (nano grados), y otras formas de adiestramiento a corto plazo y específicos a un tema ha aumentado en gran medida para reducir los costes de la educación y las oportunidades de adiestramiento para que los hombres del aire se aprovechen de ellas.[36] Más cortos en duración que un título de asociado pero de más duración que un curso de adiestramiento tradicional, los *microdegrees* y otras formas nuevas de aprendizaje basado en la *Internet* se han proliferado en años recientes. El Comando Espacial de la Fuerza Aérea debería adoptar activamente y explorar esta tendencia como una manera de adiestrar y capacitar a los hombres del aire especializados en el espacio y la cibernética. Asociaciones con compañías de aprendizaje en línea tales como *Udacity, Coursera, edX*, u otros proveedores de cursos en línea masivos y abiertos (MOOC, por sus siglas en inglés) podrían producir oportunidades para que los hombres del aire logren una educación y adiestramiento actual hecho a la medida de las necesidades del Comando Espacial de la Fuerza Aérea, con costes de inscripción y barreras de tiempo mucho más bajas para los estudiantes.[37]

La educación tradicional aún desempeña un papel muy importante, pero el Comando Espacial de la Fuerza Aérea debe tomar medidas activas para investigar cómo estas tecnologías en la educación están cambiando el mercado de la educación civil.[38] Los microdegrees pueden ofrecerle al personal de la Fuerza Aérea una forma de capacitación más ágil, actual y responsiva que también les permite permanecer al día en el campo de la tecnología de informática que avanza

rápidamente. Más allá de la educación y el adiestramiento individual, las asociaciones entre el Comando Espacial de la Fuerza Aérea y las compañías MOOC pueden ofrecer una manera relativamente económica de capacitar al personal especializado en el espacio y la cibernética en general.[39]

Inversión extensa en el cuerpo de adiestramiento en la cibernética

De todos los ámbitos bélicos, el terreno de la cibernética, que crece exponencialmente, hace que "enseñar la cibernética" sea una tarea que con el tiempo se torne en un reto. En comparación, muy poco cambia de un año a otro a medida que los pilotos reciben adiestramiento en las operaciones aéreas, o los operadores espaciales reciben adiestramiento en las operaciones espaciales, sin embargo el material del curso en el ámbito cibernético puede tornarse obsoleto en cuestión de meses.[40]

Al igual que las destrezas y conocimientos de un operador se atrofian más rápido que en otros ámbitos, también se atrofiará el material desarrollado para el adiestramiento y la educación.[41] Por cada instructor asignado a un curso de instrucción cibernética, el Comando Espacial de la Fuerza Aérea debe considerar asignar a un segundo miembro cuyas responsabilidades incluyan una revisión rápida del material del curso con base en las circunstancias cambiantes en el ámbito cibernético y ajustes basados en el rendimiento y comentarios del estudiante.

Mientras que el instructor se encarga de la instrucción, calificación y administración, un desarrollador del curso se cercioraría que la instrucción del curso fuese oportuna y relevante. Cada vez que sea posible, los desarrolladores del curso deben ser incorporados con las unidades operacionales o los socios en la industria en el sector privado durante plazos cortos de tiempo para conservar el conocimiento y las destrezas avanzadas.[42] Al igual que un sistema de informática con vulnerabilidades, los cursos de instrucción cibernética no pueden darse el lujo de permanecer estáticos; en cambio, se deben tratar como un sistema en evolución constante. Por cada cuadro de instructores, debe haber un cuadro igualmente grande o más de desarrolladores de curso que se encarguen de esta función.

Conclusión

De todos los ámbitos bélicos, el espacio cibernético es el que cambia más rápido. Estos cambios están impulsando a las misiones de la Fuerza Aérea y a los sistemas de armamento hacia una dependencia mayor en el espacio cibernético y en el espacio. Comprendiendo, anticipando y preparándose para mayores grados de dependencia en la cibernética a lo largo de la fuerza, el Comando Espacial de la Fuerza Aérea capacitará hombres del aire dedicados al espacio y la cibernética que estén preparados para prevalecer en el campo de batalla cibernético del futuro.

El Comando Espacial de la Fuerza Aérea debería estudiar las ventajas de sacarle provecho a datos grandes para la toma de decisiones, continuar desarrollando capacitación cibernética específica a la misión, hacer que el adiestramiento en cibernética esté disponible a los operadores en misiones que dependen de la cibernética, fortalecer los lazos con los socios en la industria, fomentar nuevas formas de educación y adiestramiento e invertir en gran medida en un cuadro más amplio de entrenadores especializados en el espacio cibernético. Estas inversiones, algunas pequeñas y otras grandes, rendirían dividendos considerables cuando el Comando Espacial de la Fuerza Aérea de repente se encuentre sumergido en el campo de batalla cibernético del futuro. Es posible imaginar, en algún punto en el futuro no muy distante, una Fuerza Aérea que depende completamente del espacio y del espacio cibernético. Es igualmente posible imaginar una Fuerza Aérea cuyas capacidades de defensa cibernética son mucho mayores que las nuevas amenazas que estas dependencias en el espacio y el espacio cibernético constituyen. El momento para comenzar a superar los retos de la dependencia en la cibernética es ahora. ❑

Notas

1. Los grados de dependencia en la cibernética se pueden usar para describir cualquier capacidad, tecnología o estrategia militar. La supremacía en el ámbito cibernético espacial es análoga con la supremacía aérea y el autor la define como el grado de superioridad cibernética en la que la fuerza cibernética opositora es incapaz de interferencia eficaz.

2. Las fuerzas del mercado obligarán a los mercados a asegurar y defender un espacio de batalla más grande, pero el Departamento de Defensa en sí también ampliará el espacio de batalla cibernético de una manera mucho más indirecta.

3. Joint Publication (Publicación Conjunta) (JP) 3-12 (R), *Cyberspace Operations* (Operaciones Ciberespaciales), 5 de febrero de 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. El JP 3-12 se refiere a esto como la "relación singular" entre el espacio y el espacio cibernético. El autor le llama a esto como "dependencia del ámbito en la cibernética" porque todas las operaciones en el ámbito espacial en la actualidad dependen de la supremacía del espacio cibernético.

4. Ibid.; y JP 3-14, *Space Operations*, 29 de mayo de 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

5. JP 3-12 (R), *Cyberspace Operations*, define al espacio cibernético como "muchas redes diferentes y que a menudo se superponen, al igual que nódulos (cualquier dispositivo o ubicación lógica con una dirección de protocolo de Internet (IP, por sus siglas en inglés) u otro identificador análogo) en esas redes, y el sistema de datos (tales como tablas de enrutamiento) que las apoyan". (I-2).

6. Ibid.

7. Ibid. Con respecto a las operaciones espaciales, la capa de la red física del espacio cibernético incluye los sistemas de informática con los cuales los operadores llevan a cabo las operaciones de comando y control y reciben y analizan telemetría; los circuitos que conectan esos sistemas de informática al equipo terrestre; el equipo terrestre en sí, que prepara y envía los datos al vehículo espacial; los vehículos espaciales en sí. La capa de la red lógica del espacio cibernético está incorporada en cada pedazo de la red física. Cuando los operadores espaciales cambian las configuraciones en o envían comandos a cualquier parte de la capa de la red física, cifran o descifran transmisiones, o llevan a cabo incorporación y análisis de datos, ellos están operando dentro de la capa de la red lógica del espacio cibernético. Hasta cierto grado, esas acciones pueden ser consideradas como operaciones ciberespaciales. La capa de la ciber persona describe a los operadores espaciales que dependen de las capas física y lógica de la red para llevar a cabo operaciones espaciales. La capa de la ciber persona también incluye posibles adversarios que podrían interrumpir las operaciones espaciales a través de sus propias operaciones ciberespaciales.

8. Damon Poeter, "How Moore's Law Changed History (and Your Smartphone)" (Cómo la Ley de Moore cambión la historia [y su teléfono inteligente]), PC, 19 de abril de 2015, http://www.pcmag.com/article2/0,2817,2482133,00.asp.

9. JP 3-12 (R), *Cyberspace Operations*; y Mark Pomerleau, "Army Cyber Chief Outlines Key Challenges, Goals" (Jefe de cibernética del Ejército esboza retos principales), Defense Systems, 18 de marzo de 2015, http://defensesystems.com/Articles/2015/03/18/Army-cyber-Cardon-outlines-challenges-goals.aspx.

10. Max Boot, "The Paradox of Military Technology" (La paradoja de la tecnología militar), *New Atlantis*, no. 14 (Otoño 2006): 13–32.

11. Jose Pagliery, "Love, Not War: Pentagon Courts Silicon Valley" (Amor no la guerra: El Pentágono corteja al Silicon Valley), CNN, 23 de abril de 2015, http://money.cnn.com/2015/04/23/technology/security/military-silicon-valley/.

12. Tte Cnel Gregory Conti y Cnel John "Buck" Surdu, "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?" (Ejército, Armada, Fuerza Aérea y la cibernética— ¿es hora de contar con una Sección de Guerra Cibernética en la Milicia?), *IAnewsletter* 12, núm. 1 (Primavera 2009): 14–18; y Andrew Phillips, "The Asymmetric Nature of Cyber Warfare" (La naturaleza asimétrica de la guerra cibernética), US Naval Institute, 14 de octubre de 2012, http://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare.

13. JP 3-12 (R), *Cyberspace Operations*.

14. Katia Moskvitch, "Are Drones the Next Target for Hackers?" (¿Son los aviones no tripulados el siguiente blanco de los piratas cibernéticos?) BBC, 6 de febrero de 2014, http://www.bbc.com/future/story/20140206-can-drones-be-hacked; y Aliya Sternstein, "How to Hack a Military Drone" (Cómo piratear un avión no tripulado militar), DefenseOne, 29 de abril de 2015, http://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/.

15. Christian Davenport, "Meet the Most Fascinating Part of the F-35: The $400,000 Helmet" (Conozcan la parte más fascinante del F-35: El casco de $400,000 dólares), Washington Post, 1º de abril de 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/04/01/meet-the-most-fascinating-part-of-the-f-35-the-400000-helmet/; "Insects Inspire Military Mini Drones" (Los insectos inspiran a las mini aeronaves no tripuladas), *Fox News*, 18 de septiembre de 2014, http://www.foxnews.com/tech/2014/09/18/insects-inspire-military-mini-drones/; Joyce P. Brayboy, "Army Researcher's Interest in Robots Leads to Innovative Device" (Interés de investigador del Ejército en los robots conduce a un dispositivo innovador), US Army, 2 de julio de 2015, http://www.army.mil/article/151527; Terri Moon Cronk, "Robot to Serve as Future Military's 'Pack Mule,' " (Robot sirve como "mulo de carga" de la milicia del futuro), US Department of Defense, 19 de diciembre de 2012, http://archive.defense.gov/news/newsarticle.aspx?ID=118838; Brendan McGarry, "*U.S. Military Begins Testing 'Smart' Rifles*" (Milicia de EUA comienza a probar "rifles inteligentes"), DefenseTech, 15 de enero de 2014, http://defensetech.org/2014/01/15/u-s-military-begins-testing-smart-rifles/; y Kris Osborn, "*Navy to Deploy First Underwater Drones from Submarines*" (Armada desplegará las primeras aeronaves no tripuladas bajo el agua desde submarinos), Military.com, 13 de abril de 2015, http://www.military.com/daily-news/2015/04/13/navy-to-deploy-first-underwater-drones-from-submarines.html.

16. La seguridad cibernética es más comúnmente comprendida como relacionada con el cumplimiento, tales como la gestión de vulnerabilidades y la implementación de medidas protectoras. Esto es en contraste con la defensa activa que es la

implementación de medidas o maniobras defensivas en anticipación de, durante, o después de un incidente cibernético o enfrentamiento con un adversario.

17. "*The Pentagon Got Hacked While You Were at Def Con*" (El Pentágono fue pirateado mientras usted estaba en Def Con), *Wired*, 9 de agosto de 2015, http://www.wired.com/2015/08/security-news-week-pentagon-got-hacked-def-con/; Andy Greenberg, "*Hackers Remotely Kill a Jeep on the Highway—with Me in It*" (Los piratas cibernéticos derriban un Jeep por control remoto en la carretera—conmigo adentro), *Wired*, 21 de julio de 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Kim Zetter, "*Is It Possible for Passengers to Hack Commercial Aircraft?*" (¿Es posible que los pasajeros puedan piratear una aeronave comercial?), *Wired*, 26 de mayo de 2015, http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/; y Hallie Golden, "*Security Experts Point to OPM's Biggest Cybersecurity Failure*" (Expertos en seguridad señalan el fracaso más grande de OPM en la seguridad cibernética), NextGov, 21 de julio de 2015, http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/. En cada uno de estos ejemplos, las explotaciones fueron descubiertas por investigadores de seguridad, y no piratas cibernéticos profesionales "militarizados". Si una amenaza bien organizada, avanzada y persistente comprometiese sus recursos para blancos similares, los resultados probablemente serían mucho más severos.

18. JP 3-12 (R), *Cyberspace Operations*. Tradicionalmente, la mayor parte del espacio de batalla que se puede defender en el ámbito del espacio cibernético ha sido la infraestructura de las comunicaciones que proveen apoyo a la misión principal. Una implicación de mayor dependencia en la cibernética sería que el espacio de batalla que se puede defender se ampliaría para incluir los sistemas de misión en sí. El reto es que la interrupción intuitiva y amistosa a la misión sería más probable mientras se opera defensivamente en una misión o sistema de informática que si fuese mientras se defiende la infraestructura de las comunicaciones.

19. *Recorded Future Special Intelligence Desk* (Buró especial de inteligencia de *Recorded Future*), "*Week to Weak: The Weaponization of Cyber Vulnerabilities*" (De semana a debilidad: Emplazamiento de armas de vulnerabilidades cibernéticas), Ref ID: 2014-02 (Somerville, MA: Recorded Future, 4 de diciembre de 2014), http://go.recordedfuture.com/week-to-weak-report. El informe "*Week to Weak*", publicado a fines del 2014, ilustra la velocidad rápida a la cual las vulnerabilidades son militarizadas y vistas en el estado natural. Un análisis por *Recorded Future* reveló que el número de días promedio para explotar una vulnerabilidad es solamente 7,5 días. Para referencia, el informe menciona al Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) como haber publicado 7.000 nuevas vulnerabilidades en el 2014. Esto ilustra la velocidad increíble a la cual la seguridad cibernética mide, tal como la gestión de vulnerabilidades, debe tener lugar para mantener los niveles de riesgo apropiados.

20. "*Standards Are Making the Internet of Things Come Alive*" (Las normas hacen que la *Internet* de las cosas cobren vida), IEEE Standards Association, 8 de abril de 2013, http://standardsinsight.com/ieee_company_detail/standards_iot; y Dr. W. Charlton Adams Jr., "*The Internet of Things and the Connected Person*" *Wired* "La *Internet* de las cosas y la persona conectada), diciembre de 2014, http://www.wired.com/insights/2014/12/iot-connected-person/.

21. Klint Finley, "*Hacked Fridges Aren't the Internet of Things' Biggest Worry*" (Los refrigeradores pirateados no son la mayor preocupación de la *Internet* de las cosas), *Wired*, 12 de marzo de 2015, http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/; Bill Wasik, "*In the Programmable World, All Our Objects Will Act as One*" (En el mundo programable, todos nuestros objetos actuarán como uno), *Wired*, 14 de mayo de 2013, http://www.wired.com/2013/05/internet-of-things-2/; y Dan Saffer, "*The Wonderful Possibilities of Connecting Your Fridge to the Internet*" (Las maravillosas posibilidades de conectar su refrigerador a la *Internet*), *Wired*, 29 de octubre de 2014, http://www.wired.com/2014/10/is-your-refrigerator-running/.

22. Si el público no es disuadido por inquietudes con respecto a la privacidad y la seguridad, las preferencias de los consumidores por dispositivos inteligentes, desde carros conducidos por control remoto y refrigeradores en red, deben proporcionarles a las empresas abastecedoras de una ventaja competitiva. Si este es el caso, la competencia de esas "empresas emprendedoras" podrían buscar adoptar la misma tecnología o crear una propia, posiblemente transformando la tecnología en sí y eliminando alternativas no adoptadas del mercado.

23. Cade Metz, "*Mavericks Invent Future Internet Where Cisco Is Meaningless*" (Aventureros inventan *Internet* del futuro en la que Cisco no tiene ningún significado), *Wired*, 16 de abril de 2012, http://www.wired.com/2012/04/nicira/; y Klint Finley, "*GE's New Cloud Must Be the Most Tempting Hacker Bait Ever*" (Nueva Cloud de GE tiene que ser la carnada más tentadora que nunca para los piratas cibernéticos), *Wired*, 5 de agosto de 2015, http://www.wired.com/2015/08/ges-new-cloud-may-tempting-hacker-bait-ever/.

24. En vista de que las operaciones espaciales dependen inmensamente de la supremacía del espacio cibernético, varias, pero no todas estas recomendaciones se centran en torno a la cibernética.

25. Una prueba de pericia cibernética probablemente evaluaría la solución de problemas basados en la lógica al igual que el razonamiento abstracto, dos destrezas necesarias para el éxito en el espacio cibernético (y en el espacio).

26. Críticamente, esas pruebas no se deben utilizar para afectar la selección de los campos profesionales de los individuos durante los primeros años de implementación. Con el tiempo, a medida que esas pruebas se perfeccionan y se pueden extraer conclusiones de esos puntos de datos, se tornarán útiles en tomar esas decisiones. Hacer conclusiones demasiado rápido y llevar a cabo decisiones de selección durante el proceso de perfeccionamiento sesgarían los resultados y solo conducirían a conclusiones preconcebidas en lugar de ofrecer verdaderas perspectivas.

27. Capt Kinder Blacke, "*Intermediate Network Warfare Training Up and Running*" (Entrenamiento bélico intermedio en la red está funcionando), Air Force Space Command, 3 de marzo de 2011, http://www.afspc.af.mil/news/story.asp?id=123245023; y Sgto 2º Jarrod Chavana, "*Airmen Train for 'New Wild, Wild West' in Cyber Domain*" (Suboficiales se en-

trenan para el "nuevo oeste salvaje" en el ámbito cibernético), *Santa Maria Times*, 10 de octubre de 2014, http://santamariatimes.com/news/local/military/airmen-train-for-new-wild-wild-west-in-cyber-domain/article_1633ec02-eb22-54e5-ad04-f4bea53b776c.html.

28. "National Cybersecurity Workforce Framework" (Estructura de la fuerza laboral de la seguridad cibernética nacional), *National Initiative for Cybersecurity Education* (Iniciativa Nacional para la Educación en Seguridad Cibernética), consultada el 15 de octubre de 2015, http://csrc.nist.gov/nice/framework/.

29.Además de estar informados por los estándares de NIST, el adiestramiento inicial e intermedio para los suboficiales de la Fuerza Aérea debe ser informado por técnicas de operaciones utilizadas en la comunidad conjunta, tales como el proceso de planificar, informar, ejecutar y pos informar (PBED, por sus siglas en inglés).

30. J. R. Wilson, "*Interview: Col. Robert 'Shark' Garland, Commandant, USAF Weapons School*" (Entrevista: Cnel Robert "Shark" Garland, Comandante, Escuela de Armamento de la USAF), Defense Media Network, 6 de noviembre de 2011, http://www.defensemedianetwork.com/stories/interview-col-robert-%E2%80%9Cshark%E2%80%9D-garland-commandant-usaf-weapons-school/.

31. El ingreso al programa y la asignación después del programa podría ser administrado de manera muy similar a los procedimientos de la Escuela de Armamento de la USAF, sin necesidad de crear todo un programa de adiestramiento separado de los cursos cibernéticos tradicionales intermedios y avanzados que son específicos a la misión del egresado.

32. Jim Garamone, "*Winnefeld: DoD Must Strengthen Public, Private Ties*" (Winnefeld: El Departamento de Defensa debe fortalecer los lazos públicos y privados), US Department of Defense, 14 de mayo de 2015, http://www.defense.gov/news/newsarticle.aspx?id=128810; y Kevin Gilmartin, "*Education with Industry Program Offers Different Perspective*" (La educación con el programa de la industria ofrece una perspectiva diferente), Air Force Print News, 14 de marzo de 2008, http://www.hanscom.af.mil/news/story_print.asp?id=123090306.

33. Cheryl Pellerin, "*Carter Seeks Tech-Sector Partnerships for Innovation*" (Carter busca asociaciones con el sector técnico para la innovación), US Department of Defense, 23 de abril de 2015, http://www.defense.gov/news/newsarticle.aspx?id=128655.

34. Mark Pomerleau, "*Carter Details DoD's Innovation Plans*" (Carter detalla planes del innovación del DOD), Defense Systems, 6 de mayo de 2015, https://defensesystems.com/articles/2015/05/06/carter-dod-innovation-plans-congress.aspx; y Patrick Tucker, "*Pentagon Sets Up a Silicon Valley Outpost*" (Pentágono establece puesto de avanzada en *Silicon Valley*), Defense One, 23 de abril de 2015, http://www.defenseone.com/technology/2015/04/pentagon-sets-silicon-valley-outpost/110845/.

35. Pomerleau, "Carter Details DoD's Innovation Plans."

36. Stuart M. Butler, "*How Google and Coursera May Upend the Traditional College Degree*" (Cómo *Google* y *Coursera* podrían afectar las carreras universitarias), Brookings Institution, 23 de febrero de 2015, http://www.brookings.edu/blogs/techtank/posts/2015/02/23-mooc-google-coursera-butler/.

37. Ibid.

38. Además de asociarse con las compañías en sí, el análisis de la tecnología subyacente y los métodos podrían ilustrar eficiencias que podrían implementarse en cursos dictados a cabo por militares.

39. Jeffrey R. Young, "*Will MOOCs Change the Way Professors Handle the Classroom?*" (¿Podrían los MOOC cambiar la manera como los profesores manejan los salones de clase?), *Chronicle of Higher Education*, 7 de noviembre de 2013, http://chronicle.com/article/Will-MOOCs-Change-Campus/142869/.

40. Conti y Surdu, "Army, Navy, Air Force, and Cyber," 14–18.

41. Ibid.

42. De cuando en cuando, los instructores y los desarrolladores de cursos deben cambiar sus respectivas funciones para mantenerse actualizados.

Subteniente (2nd Lt) Christopher Babcock, USAF (BS, Indiana University) es Comandante de Tripulación y Subjefe de Sección para la Red de Control de Satélites de la Fuerza Aérea, del 50º Escuadrón de Comunicaciones Espaciales. Es oficial de operaciones ciberespaciales con interés especial en la defensa de la red e integración de inteligencia.