(Foto: Fuerza Aérea de EUA, Aerotécnico Franklin R. Ramos)

Sargento segundo Jerome Duhan, Fuerza Aérea de EUA, un administrador de redes con el 97º Escuadrón de Comunicaciones, inserta un disco rígido en el servidor de retina en el centro de control de red, 24 de enero de 2014, en la Base Aérea Altus, estado de Oklahoma, en preparación para una inspección de presteza cibernética del comando.

La fuerza cibernética de EUA

La próxima guerra

Mayor Matt Graham, Ejército de EUA

En el libro *Wealth of Nations* [La riqueza de las naciones], publicado en 1776, Adam Smith explica cómo la división del trabajo permite el mayor nivel de eficacia: los agricultores se centran en la producción de comestibles, los herreros se enfocan en la producción de bienes de metal, etcétera[1]. Este principio aún es válido hoy en día, las personas y organizaciones desarrollan la pericia al centrarse en una sola actividad. En las fuerzas armadas de EUA, la división del trabajo entre las distintas instituciones militares logran esta

pericia: la Fuerza Aérea se centra en la superioridad aérea, permitiendo que el Ejército se enfoque en la guerra terrestre y que la Armada se preocupe con el combate marítimo. El Cuerpo de Infantería de Marina desarrolla su pericia en cerrar la brecha entre la tierra y el mar.

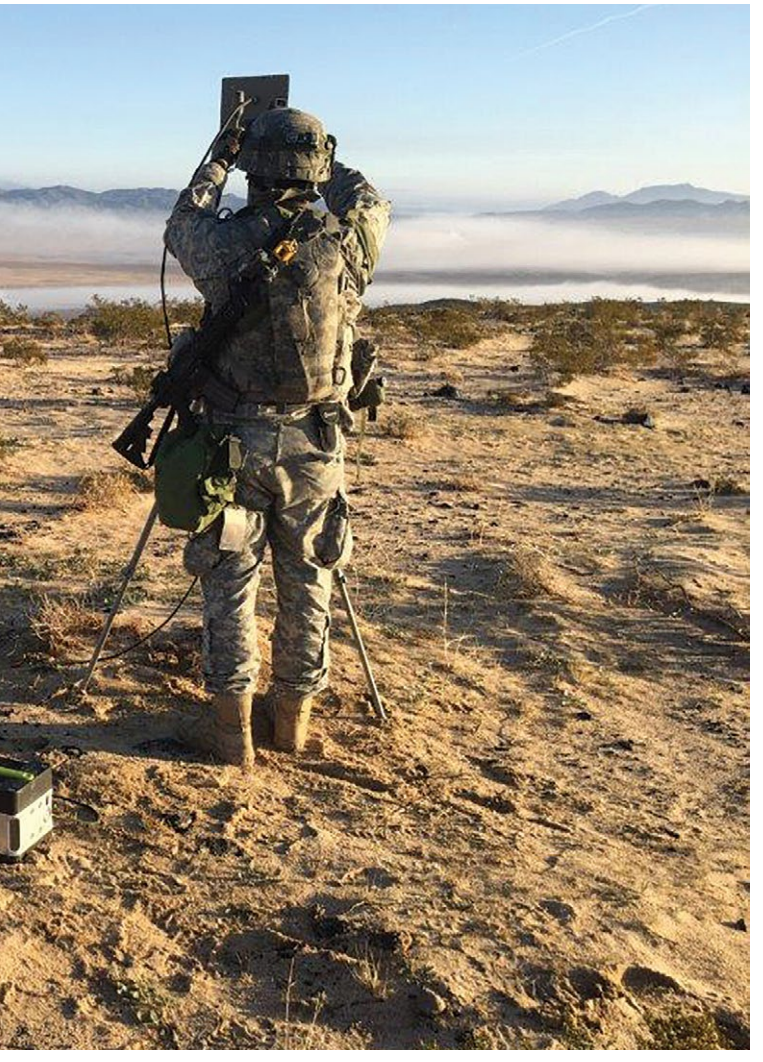
Si bien posee algunas características muy distintas de los dominios físicos, el ciberespacio recientemente ha surgido como un dominio independiente que requiere su propia pericia militar especial. Con las naciones buscando ventajas en este nuevo dominio, la competencia en el ciberespacio ha asumido muchas características de la guerra y, hoy en día, requiere el mismo nivel de pericia que se necesita para ganar las guerras en el mundo. Las fuerzas armadas necesitan una Fuerza Cibernética de EUA, igual al Ejército, Armada, Fuerza Aérea y el Cuerpo de Infantería de Marina, para centrarse en el dominio de ciberespacio.

El planteamiento actual en el ciberespacio

Las fuerzas armadas no han estado de brazos cruzados durante el comienzo y desarrollo del ciberespacio y guerra cibernética. El Departamento de Defensa (DOD) estableció el Comando Cibernético de EUA (USCYBERCOM) en 2009 como un cuartel general conjunto para organizar los esfuerzos del departamento en el ciberespacio. Integrantes de todas las instituciones armadas se unen en el USCYBERCOM para enfrentar las amenazas del ciberespacio. Una parte del presupuesto del DOD se asigna directamente al USCYBERCOM y algunos recursos vienen de las instituciones armadas. Bajo el USCYBERCOM, cada institución estableció un cuartel general de componente (p.ej. el Comando Cibernético del Ejército o el Comando Cibernético de la Flota) para apoyar los esfuerzos del DOD en el ciberespacio. Sin lugar a dudas, la importancia emergente del ciberespacio merece todas estas acciones. Sin embargo, cada institución militar que dedica una fracción de su atención al ciberespacio garantiza dos resultados: las instituciones armadas están distraídas de sus papeles de combate tradicionales en los dominios físicos y los esfuerzos de ciberespacio son ineficaces (en el mejor de los casos), desarticulados (probablemente) o fratricidas (en el peor de los casos). Actualmente, esta ineficacia no es una gran preocupación y acaba en gran parte en frustración burocrática. Sin embargo, cuando haya mucho más en juego y los guerreros cibernéticos tengan que demostrar que son mejores que los guerreros cibernéticos de los adversarios, estas ineficacias no serán tolerables.

El planteamiento actual (con cada institución armada haciendo su contribución al esfuerzo conjunto en el ciberespacio) no solo es ineficaz, sino también innecesario. Una operación en el ciberespacio es, en gran parte, independiente de la plataforma o dominio físico desde los cuales un guerrero cibernético gana acceso al ciberespacio. La lógica usada o la vulnerabilidad de redes explotada por un guerrero cibernético es la misma ya sea si es ejecutada desde puente de un portaaviones, dentro de un avión de mando y control o un escritorio en un complejo de oficinas con aire acondicionado.

En una operación de ciberespacio, lo decisivo es la explotación de las vulnerabilidades en un sistema del adversario antes de que el adversario pueda identificarlas y mitigarlas (y vice versa). Cuando lo considera de esta manera, los guerreros cibernéticos de la Armada y Fuerza Aérea comparten más similitudes con sus guerreros cibernéticos homólogos que con



(Foto: Ejército de EUA)

Soldados de la 780ª Brigada de Inteligencia Militar realizan operaciones de ciberespacio durante una rotación de entrenamiento con el 2º Equipo de Combate de Brigada Stryker de la 2ª División de Infantería en el Centro Nacional de Adiestramiento en el Fuerte Irwin, estado de California, 24 de enero de 2016. La unidad, basad en el Fuerte Meade, estado de Maryland, fue una de varias organizaciones cibernéticas que participaron en la rotación como parte de un programa experimental concebido para fortalecer y usar las capacidades cibernéticas en sus formaciones tácticas.

otros marineros y aerotécnicos de sus respectivas instituciones armadas.

La Fuerza Cibernética de EUA proporcionaría el enfoque

A diferencia del planteamiento que el DOD usa actualmente, un servicio cibernético independiente proporcionaría el nivel necesario de concentración en las operaciones en el ciberespacio. Se requiere un mayor nivel de concentración para desarrollar la competencia de ciberespacio en todas las fuerzas armadas y podría anticiparse avances especiales en tres áreas: el desarrollo de liderazgo, la formación de guerreros cibernéticos y las operaciones en el ciberespacio.

El liderazgo. La Fuerza Cibernética de EUA garantizaría que los líderes de ciberespacio de mayor jerarquía posean experiencias profundas en las operaciones de ciberespacio. Actualmente, los oficiales de mayor jerarquía en cada una de las instituciones armadas ascienden en grado por el rendimiento en el dominio de su institución (p.ej. el jefe de la Fuerza Aérea es un piloto de avión caza y el jefe de operaciones navales es un oficial de submarino). Es conveniente que estos oficiales tienen experiencias de guerra en sus dominios. Deben comunicar los desafíos relacionados con sus dominios a los encargados de tomar decisiones políticas. Luego, estos líderes interpretan la orientación política y distribuyen los fondos a sus instituciones. ¿Quién cumple esta función para el dominio de ciberespacio? El comandante del USCYBERCOM actualmente aboga por el ciberespacio. Sin embargo, el USCYBERCOM es subordinado al Comando Estratégico de EUA (USSTRATCOM), separados por varios niveles de los encargados de tomar decisiones políticas. Además, el comandante del USCYBERCOM asciende al mando desde una de las instituciones armadas, en gran parte gobernada por oficiales que se centran en sus dominios físicos específicos. Dado que las instituciones militares determinan cuáles oficiales van a ascenderse, aun el comandante del USCYBERCOM debe dividir su atención entre el ciberespacio y el dominio de su institución armada o correr el riesgo de no avanzar en su carrera. El establecimiento de una Fuerza Cibernética, junto con un representante en el Estado Mayor Conjunto, permitiría que los líderes militares con una profundidad de experiencias prácticas en el ciberespacio comuniquen los desafíos de la guerra cibernética a los que toman decisiones políticas. A su vez, los líderes de la Fuerza Cibernética podrían emplear eficazmente la orientación y recursos atribuidos a las operaciones militares en el ciberespacio.

Los guerreros cibernéticos. Además de la formación de líderes experimentados para la guerra cibernética, la Fuerza Cibernética atraería y formaría a guerreros cibernéticos más capacitados. Actualmente, los civiles que desean defender la nación en el ciberespacio tienen que optar por una de las instituciones armadas existentes y someterse al currículum de su entrenamiento básico. Si bien estos programas son exquisitamente adaptados para formar a soldados, marineros aerotécnicos e integrantes del Cuerpo de Infantería de Marina, pueden ser innecesarios e intimidantes a los civiles que solo desean participar en la competencia predominantemente mental de la guerra cibernética. Sin lugar a dudas, el DOD emplea a muchos civiles que participan en las actividades en el ciberespacio; sin embargo, esta es una solución por debajo de lo ideal. Hay complicaciones legales con los civiles que llevan a cabo actividades de guerra y el reclutamiento de guerreros cibernéticos para servir como integrantes militares reconoce con más precisión sus contribuciones y permite un mayor nivel de movilidad económica y mando. Con el establecimiento de la Fuerza Cibernética, las fuerzas armadas reclutarían y clasificarían a los guerreros cibernéticos sin disuadir a los civiles interesados y, en su lugar, influenciaría a estas personas a entrar en las industrias lucrativas de la informática o comunicaciones.

(Imagen: CERDEC)

Los límites entre las amenazas cibernéticas tradicionales y las amenazas tradicionales de guerra electrónica se han desvanecido. El programa Guerra Cibernética y Electrónica Integrada del Centro de Comunicaciones-Investigación, Desarrollo e Ingeniería de Electrónica del Comando de Pertrechos Militares del Ejército de EUA usa tanto las capacidades cibernéticas y de guerra electrónica como un sistema integrado para incrementar la conciencia situacional del comandante.

El entrenamiento de los guerreros cibernéticos también llegaría a ser más eficaz en la Fuerza Cibernética. Actualmente, cada institución armada crea un programa de entrenamiento para sus guerreros cibernéticos respectivos. Por ejemplo, el Ejército estableció el Centro Cibernético de Excelencia en el Fuerte Gordon, en el estado de Georgia. Este método distribuido para formar a guerreros cibernéticos casi garantiza la ineficacia en la iniciativa más amplia de ciberespacio del DOD. Si bien el USCYBERCOM trabaja para establecer estándares comunes en el entrenamiento de todas las fuerzas armadas, las interpretaciones de las distintas instituciones armadas diferirán, aunque ligeramente. Los profesores en cada uno de estos centros producirán resultados diferentes. Por ejemplo, el Ejército podría emplear al mejor entrenador de código de computadoras, mientras que el Cuerpo de Infantería de Marina podría emplear al mejor entrenador de redes. A pesar de los estándares de entrenamiento comunes, las interpretaciones divergentes y variación de destrezas de los instructores producirán guerreros cibernéticos de calidad subóptima. Por el contrario, la Fuerza Cibernética podría consolidar los mejores profesores en un solo centro de entrenamiento de ciberespacio y supervisar mejor la implementación de estándares. Además, dado que los estudiantes estarían consolidados, los más brillantes podrían interactuar el uno con el otro y el cuerpo docente podría facilitar un mayor nivel de investigación de ciberespacio.

La formación continúa más allá del entrenamiento. Los trabajos de clase y la práctica comienzan donde termina el entrenamiento. Como una institución independiente, la Fuerza Cibernética podría adaptar

(Foto: Ejército de EUA, Sgto. 2º Chuck Burden)

El Jefe de Estado Mayor del Ejército, general Mark Milley, observa mientras oficiales del Instituto Cibernético del Ejército en la Academia Militar de EUA en West Point, estado de Nueva York, demuestran el derribo de una aeronave no tripulada con fusil con capacidad cibernética, 12 de octubre de 2015.

diestramente la formación profesional de sus guerreros cibernéticos. Podrían establecerse campos de estudio (p.ej. codificación, redes, protección contra virus o gestión de intrusión) y también podrían diseñarse trayectorias profesionales, incluyendo las asignaciones en unidades de ciberespacio, en agencias de desarrollo de capacidades y en estados mayores conjuntos, donde podrían integrarse los efectos de ciberespacio con las operaciones en los dominios físicos. Actualmente, los guerreros cibernéticos dependen de las necesidades de recursos humanos de sus instituciones militares y, frecuentemente, estas personas se consideran intercambiables con el personal de comunicaciones. Si bien hay actividades que coinciden indudablemente entre los campos de comunicaciones y la guerra cibernética, una fuerza cibernética podría posibilitar un mejor discernimiento de pericias y mejor gestión de capital humano.

Operando en el ciberespacio. La ventaja principal de establecer una Fuerza Cibernética independiente es la capacidad de desarrollar la fuerza más capaz. Sin embargo, las operaciones en el ciberespacio también llegarán a ser menos arriesgadas y más eficaces. En los dominios físicos, es relativamente fácil dividir el campo de batalla por lugar físico: el Ejército opera tierra adentro, la Armada opera en el mar, el Cuerpo de Infantería de Marina opera en las costas y la Fuerza Aérea en los cielos. Sin embargo, tales límites obvios no existen en el ciberespacio y las cuatro fuerzas armadas operan en todas partes del mismo. La oportunidad para que una institución infrinja en la operación de otra en el ciberespacio, o accidentalmente la sabotee, es más probable que en los dominios físicos separados. La carga de mando y control y el riesgo de fratricidio en el ciberespacio incrementan con el número de guerreros cibernéticos de cuatro fuerzas armadas distintas que operan independientemente en el dominio. Otra consecuencia de tener cuatro iniciativas distintas en el ciberespacio es el potencial para la redundancia imprevista (p.ej., dos instituciones podrían dedicar recursos a resolver el mismo problema o desarrollar la misma capacidad). Una

(Foto: Agencia Nacional de Seguridad)

El Comando Cibernético de EUA se encuentra en el Fuerte Meade, estado de Maryland, junto con la sede de la Agencia Nacional de Seguridad y Servicio Central de Seguridad.

iniciativa de supervisión conjunta podría reducir parte de la redundancia, pero más burocracia agrega tiempo y dinero a un proceso de desarrollo de capacidades que ya requiere mucho tiempo. Sacar las cuatro fuerzas armadas de la lucha por el ciberespacio disminuye el riesgo de pisar el uno al otro y malgastar los recursos.

Las ventajas para las fuerzas armadas. En su libro *Good to Great*, Jim Collins moderniza algunos de los pensamientos de Adam Smith y observa que las empresas exitosas se adhieren a sus conceptos centrales, renunciando a las distracciones. Collins ofrece tres preguntas para ayudar a determinar el concepto central de una empresa: ¿Por qué siente pasión profunda? ¿En qué desempeño puede ser el mejor en el mundo? ¿Qué impulsa su motor económico?[2] Si bien es difícil traducir la última pregunta para el sector público, las primeras dos ayudan a revelar porqué el ciberespacio no debe ser una capacidad central de las fuerzas armadas existentes. Es difícil imaginar a la Armada como el mejor en el mundo en la guerra cibernética al mismo tiempo que es el mejor en la guerra marítima. Del mismo modo, pocos integrantes del Cuerpo de Infantería de Marina se describen como profundamente apasionados por la guerra cibernética. El carácter delicado y distante de la guerra cibernética va en contra de la cultura del Cuerpo de Infantería de Marina de la lucha cercana y personal. Al deshacerse de la distracción de la guerra cibernética y pasarla a la nueva Fuerza Cibernética, las fuerzas armadas actuales mantienen su enfoque en los dominios específicos.

Como una institución armada, la Fuerza Cibernética podría proporcionar fuerzas a todos los comandos de combate (CCMD) en la forma de un Comando Componente del Servicio Cibernético (CSCC). De la misma manera que los componentes de las existentes fuerzas armadas frecuentemente sirven como componentes funcionales de propósito doble (p. ej., un comando de componente de servicio de la Fuerza Aérea también puede servir como un comando de componente aéreo de fuerza conjunta), el CSCC llevaría las responsabilidades funcionales de la guerra cibernética. La Fuerza

Cibernética podría equipar a todos los CCMD con un CSCC que se centra en los sistemas del área de responsabilidad de dicho CCMD. El CSCC del USSTRATCOM podría servir como un sincronizador global de amenazas que cruzan las áreas de responsabilidad y el CSCC del Comando de Operaciones Especiales (USSOCOM) podría proporcionar guerreros cibernéticos capaces de infiltración para lograr el acceso directo a los sistemas de circuito cerrado del adversario. Si bien posiblemente fuera del alcance del DOD, el CSCC del Comando de Transporte de EUA podría intentar endurecer los sistemas de los socios de transporte clave en el ciberespacio o USSOCOM. Elevar el USCYBERCOM al nivel de CCMD sería un paso intermedio oportuno, y probable, para establecer una Fuerza Cibernética independiente. Esta medida podría quitar una capa jerárquica entre el USCYBERCOM y los encargados de tomar decisiones políticas. Además, el USSOCOM cuenta con bastante influencia en la formación de operarios especiales de las fuerzas armadas. Sin embargo, esta configuración solo resuelve parte del problema. Como un CCMD, el USCYBERCOM aún dependería de las existentes fuerzas armadas para llevar a cabo sus operaciones. Los guerreros cibernéticos aún enfrentarían

(Foto: Ejército de EUA, David Vergun)

El 2º Equipo de Combate de Brigada Blindada de la 1ª División Blindada participan en una Evaluación de integración de redes (NIE) 16.1 en el cuartel general y centro de operaciones de la brigada en el Fuerte Bliss, estado de Texas. En el ejercicio, que se llevó a cabo de 25 de septiembre a 8 de octubre de 2015, se evaluó una red que vinculó a todas las redes distintas de catorce ejércitos que participaron en vivo o virtualmente en un ambiente de combate simulado. Las nuevas tecnologías que fueron evaluadas durante la NIE 16.1 incluyeron las capacidades de red de la coalición, puestos de mando expedicionarios, capacidades de energía operativas y la creación de equipos tripulados/no tripulados (la robótica aérea y terrestre).

(p.ej, camiones comerciales de contenedores, controladores de tráfico aéreo o socios ferroviarios clave), ayudando a la fuerza conjunta a superar los desafíos que dificultan el acceso. La administración de una fuerza cibernética es mucho más fácil y más eficaz que la contribución de fuerzas de las existentes instituciones armadas al USCYBERCOM, que luego tiene que improvisar unidades cibernéticas y asignarlas con los CCMD.

Otro planteamiento para incrementar la eficacia. Un tercer planteamiento, distinto del método actual del DOD o una institución cibernética completamente independientemente, implicaría elevar el USCYBERCOM al nivel de un CCMD funcional, igual al USSTRATCOM la decisión de cuál de los trámites de ciberespacio de las fuerzas armadas podrían navegar a fin de trabajar con el USCYBERCOM. Esta configuración funciona en el USSOCOM porque el entrenamiento para un piloto de avión tipo AC-130 de la Fuerza Aérea es distinto del de un integrante de las fuerzas especiales navales (SEAL), que también es diferente del de un soldado de las fuerzas especiales del Ejército; pero no es así en el ciberespacio. Una operación de ciberespacio es la misma sin importar el dominio físico desde el cual se inicia. La solución que proporciona las unidades mejor dotadas, entrenadas y equipadas al DOD es una fuerza de ciberespacio independiente.

El establecimiento de la Fuerza Cibernética de EUA: Después de la próxima guerra

Con tantas razones que apoyan el establecimiento de la Fuerza Cibernética de EUA, ¿Qué lo impide? Hay dos obstáculos mayores. En primer lugar, el ciberespacio no ha sido confirmado como una zona de combate en el pensamiento de muchos líderes de seguridad de mayor jerarquía. En segundo lugar, a falta de una amenaza de seguridad significativa y evidente, seguirán indisponibles los recursos de seguridad nacional necesarios para hacer este tipo de gran revisión general. El próximo gran conflicto de Estados Unidos probablemente eliminará estos dos obstáculos.

Cómo demostrar que el ciberespacio es una zona de combate. El dominio aéreo jugó un rol en la Primera Guerra Mundial. Los globos de observación y combates aéreos (guerra aérea al estilo del Barón Rojo) sirven como las características predominantes de este conflicto. Sin embargo, los combatientes de la Segunda Guerra Mundial verdaderamente comprendieron la importancia de la superioridad aérea. La Batalla de Inglaterra, la campaña de bombardeo estratégico de los Aliados, el establecimiento de unidades de paracaídas y, al final, los bombardeos de Hiroshima y Nagasaki demostraron la importancia del combate en los cielos.

Actualmente, el ciberespacio se encuentra en el tipo de limbo que la potencia aérea ocupó en los años de entreguerras. Sin embargo, ha habido casos aislados de guerra cibernética entre Estados. En abril de 2007, Rusia llevó a cabo un ataque eficaz de negación de servicio contras redes principales de Estonia, paralizando muchas funciones económicas y gubernamentales de este gobierno[3]. Rusia también atacó a Georgia a través del ciberespacio, al mismo tiempo que invadió a Osetia del Sur en 2008[4]. Además, los gobiernos usan el ciberespacio para penetrar rutinariamente las redes y robar planes de misiles, fórmulas químicas y datos financieros[5]. Sin embargo, parecidas a la potencia aérea en 1920, las operaciones en el ciberespacio jugaron un rol relativamente pequeño en las últimas guerras de Estados Unidos y algunos escépticos aún consideran el ciberespacio como un entorno de aficionados o *el dominio que puede apagarse*.

Las actividades en el ciberespacio tienen un impacto cada vez más grande en las operaciones cotidianas de las Fuerzas Armadas de EUA y la economía de Estados Unidos, junto con las operaciones de sus aliados y adversarios (tanto estatales como no estatales). En la próxima guerra, el ciberespacio probablemente desempeñará un papel más prominente del que ha desempeñado en los conflictos previos. Aunque Estados Unidos gane o pierda las batallas de ciberespacio en la próxima guerra, la importancia de estos enfrentamientos justificaría el establecimiento de la Fuerza Cibernética. Si los guerreros cibernéticos de EUA logran la victoria, como hicieron los aviadores en los cielos de Europa en 1944, el ciberespacio habrá demostrado ser un dominio legítimo de guerra y el caso para una Fuerza Cibernética de EUA independiente será validado. Si Estados Unidos no logra la superioridad en el ciberespacio y sufre las consecuencias sofocantes, las ineficacias en el planteamiento actual del DOD con respecto al ciberespacio serán subrayadas y una fuerza cibernética servirá como el remedio.

Carl von Clausewitz observó que la guerra requiere el uso máximo de fuerza que una nación puede agrupar: «Si una parte usa la fuerza sin escrúpulos... mientras la otra parte se abstiene, la primera obtendrá la ventaja»[6]. Concentrar la fuerza máxima contra el enemigo, incluyendo los efectos logrados a través del ciberespacio, es la manera más segura para garantizar el éxito y la organización ineficaz dificultará este esfuerzo.

Nuevas guerras, nuevos presupuestos. Hay una dinámica extraña en las organizaciones; cuando son grandes los presupuestos, sus líderes priorizan el crecimiento sobre la eficacia. Luego, cuando disminuyen los presupuestos y verdaderamente se necesita la eficacia, no está disponible el capital necesario para optimizar las prácticas. Con un dividendo de paz como la meta, los recursos necesarios para establecer una nueva institución más eficaz no están disponibles. A medida que acaban las guerras de la década pasada, del mismo modo, los presupuestos de defensa disminuirán. Lo cierto es que el presupuesto de defensa disminuyó después de la Segunda Guerra Mundial y la Nación aún pudo establecer la Fuerza Aérea. En esta situación, los líderes de política de seguridad nacional identificaron la creciente amenaza comunista como la justificación para los gastos. Hoy en día, después de las guerras en Irak y Afganistán, no ha surgido ninguna amenaza identificable para convencer a la Nación de demorar el dividendo de paz. Por lo tanto, lograr la eficacia con el establecimiento de una institución cibernética independiente

debe esperar hasta que los fondos estén disponibles. Estos recursos de defensa probablemente estarán disponibles cuando el ciberespacio demuestre su viabilidad como un dominio de guerra en el próximo conflicto de mayor envergadura de Estados Unidos.

Conclusión

Estados Unidos necesita una institución militar independiente que se centre en el ciberespacio pero probablemente esperará hasta que comience el próximo gran conflicto para establecerla. El planteamiento actual del DOD con respecto al ciberespacio, donde las existentes fuerzas armadas donan personal con diversos grados de experiencia para que el USCYBERCOM los integre, está lleno de ineficacias. El establecimiento de una Fuerza Cibernética permitiría que prospere la comunidad de guerreros cibernéticos y quitaría la carga a las fuerzas armadas existentes de la distracción del ciberespacio. El siguiente gran conflicto de Estados Unidos permitirá que los guerreros cibernéticos demuestren la importancia de su entorno y proporcionará a las fuerzas armadas los recursos para apoyar una gran revisión burocrática.

La predicción de que será necesario tener otro conflicto para establecer una fuerza cibernética es solo una suposición basada en el probable curso de los acontecimientos. El liderazgo inspirado puede acelerar la formación de una nueva institución militar.

Clausewitz compara la guerra con la lucha libre, observando que la meta «*inmediata* de un luchador es *derribar* a su oponente para que no pueda presentar más resistencia [énfasis original]»[7]. Él observa que si un luchador usa todo su poder para inmovilizar a su oponente, el beligerante inmovilizado tal vez nunca llegue a tener la oportunidad de recuperar su fuerza total. Debido a su aislamiento por dos océanos, Estados Unidos históricamente ha tenido el lujo de reunir su fortaleza militar antes de comprometerse a la guerra. Sin embargo, los océanos no significan mucho en el ciberespacio y Estados Unidos, sin preparación, podría sufrir graves daños en los primeros ataques en el ciberespacio durante la próxima guerra de gran envergadura. Los líderes de defensa sabios comenzarán avanzando a las fuerzas armadas hacia el establecimiento de la Fuerza Cibernética de EUA para lograr un enfoque superior y eficacias antes del siguiente conflicto en lugar de después del mismo. ■

El mayor Matt Graham es un estratega del Ejército de EUA asignado a la Dirección de Estado Mayor Conjunto para el Desarrollo de Fuerzas Conjuntas. Cuenta a su haber con una maestría en Administración Pública de la Universidad de George Washington y una licenciatura en Ciencias de Computación de la Academia de la Fuerza Aérea de EUA. Sus previas asignaciones incluyen destinos en el estado de Alaska, Alemania, Washington, D.C., Irak y Afganistán.

Referencias bibliográficas

1. Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations: A Selected Edition*, editora Kathryn Sutherland (Oxford, Reino Unido: Oxford University Press, 2008), págs. 12–14.

2. Jim Collins, *Good to Great: Why Some Companies Make the Leap… and Others Don't* (Nueva York: Harper Collins Publishers, 2001), págs. 94–96.

3. Scheherazade Rehman, «Estonian's Lessons in Cyberwarfare», sitio web de U.S. News and World Report, 14 de enero de 2013, accedido 22 de agosto de 2014, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare.

4. E. Lincoln Bonner III, «Cyber Power in 21st-Century Joint Warfare», *Joint Force Quarterly* 74 (2014): p. 102.

5. Michael Riley, «How Russian Hackers Stole the Nasdaq», sitio web de Bloomberg Business, 17 de julio de 2014, accedido 4 de marzo de 2016, http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

6. Carl Von Clausewitz, *De la guerra*, editores y traductores Michael Howard y Peter Paret (Princeton, Nueva Jersey: Princeton University Press, 1989), págs. 75-76.

7. Ibíd., p. 75.