Garantizar las misiones fundamentales de la USAF en la era de la Información

Teniente General William J. Bender, USAF
Coronel William D. Bryant, USAF

La Fuerza Aérea de los Estados Unidos fue indiscutiblemente la fuerza aérea más importante y poderosa del mundo en la era industrial. Nuestro reto y oportunidad es transformar esa efectividad y capacidad para defender nuestra nación en la era de la información. Para lograrlo, debemos ser capaces de realizar nuestras cinco misiones fundamentales: superioridad aérea y espacial; inteligencia, vigilancia y reconocimiento (ISR); movilidad global rápida; ataque global; y comando y control en y a través del ciberespacio. Aunque el entorno ha cambiado de forma continua y rápida en el transcurso de la historia, estas misiones permanentes siguen siendo nuestro foco. Siempre hemos tenido que proteger y defender nuestra capacidad de lograr estas misiones; lo que ha cambiado es la necesidad de protegerlas y asegurarlas mediante el dominio del ciberespacio en la era de la información.

La libertad de acción en el ciberespacio mediante la aplicación de garantía de misión es una condición indispensable para el éxito de la ejecución de la misión fundamental de la Fuerza Aérea. Obtener y preservar la libertad de acción evitará que el enemigo interfiera de forma efectiva con las operaciones. El hacerlo también permite que la Fuerza Aérea aplique poder de combate preciso explotando las características únicas del ciberespacio. Con frecuencia no hay un buen entendimiento del ciberespacio, y sus características únicas pueden causar mucha confusión en cuanto a la forma de asegurar mejor nuestras misiones fundamentales en el ciberespacio.

El Estado Mayor define el ciberespacio como "el dominio global dentro del entorno de información formado por la red interdependiente de infraestructuras de informática y los datos residentes, que incluyen Internet, redes de telecomunicaciones, sistemas de computadoras y, procesadores y con-

troladores integrados".[1] Esta definición aclara que el ciberespacio es mucho más que simplemente las redes de computadoras tradicionales. Aunque Internet es parte del ciberespacio, ésta no constituye todo el ciberespacio. Cualquier sistema de computadoras capaz de comunicarse en alguna forma con otros sistemas de computadoras, es parte del ciberespacio. Una computadora de escritorio, una computadora de aviónica en una aeronave, un teléfono inteligente, un controlador industrial, y los procesadores en un auto moderno son parte del ciberespacio, aunque solo algunos de ellos están conectados a Internet de forma continua. La mayoría de equipos militares —desde un modesto camión hasta un bombardero B-2— tiene alguna forma de procesador y por lo tanto depende del mismo y es parte del ciberespacio.

El ciberespacio presenta la singularidad de que es una creación del hombre y se puede cambiar y modificar más fácilmente que los dominios físicos de tierra, mar, aire y espacio. Gregory Rattray ha señalado que mientras que los combatientes no pueden mover montañas y océanos, en el ciberespacio un combatiente puede mover y hasta desactivar las características geográficas equivalentes con solo tocar un conmutador.[2] Esta capacidad de mutación extrema ha originado que algunos analistas consideren al espacio como un dominio puramente virtual, pero esto es un error crítico.

El ciberespacio está compuesto de información y conexiones en un espacio virtual, pero está anclado al mundo físico.[3] Según Paul Rosenzweig, analista del ciberespacio, "Nunca debemos olvidar que el dominio cibernético es un dominio artificial creado por el hombre, solo existe en el contexto del dominio natural fundamental del mundo".[4] Los eventos en el mundo físico afectan al ciberespacio. Si el corazón del ciberespacio son las conexiones entre dispositivos de computación, cualquier cosa que afecte a esos dispositivos, o sus conexiones, altera al ciberespacio. Una unidad de aire acondicionado descompuesta en una granja de servidores, una retroexcavadora que corta un cable de fibra, o un ancla que arrastra un cable submarino puede tener un tremendo efecto en el terreno digital. Muy importante para garantizar las misiones fundamentales de la Fuerza Aérea es el entendimiento compartido de las dependencias entre el ciberespacio y los componentes físicos.

Cada uno de los sistemas críticos que ayudan al cumplimiento de nuestras misiones fundamentales se basa en las capacidades del ciberespacio. Las aeronaves, satélites, camiones y misiles balísticos intercontinentales dependen de nuestra capacidad de maniobrar y operar dentro del ciberespacio. Algunos analistas sugieren que no hay tal cosa como maniobrar en el ciberespacio ya que las computadoras simplemente ejecutan sus instrucciones, incluso si esas instrucciones incluyen la capacidad de responder a estímulos. Aunque las computadoras no maniobran, la gente sí lo hace, y el conflicto en el dominio del ciberespacio se lucha utilizando una combinación de silicio inflexible y personas flexibles que le indican al silicio lo que debe hacer. Por consiguiente, el conflicto en el dominio del ciberespacio sigue siendo controlado por seres humanos que toman decisiones y reaccionan ante los adversarios de maneras que aún serían conocidas para Clausewitz y otros pensadores militares tradicionales.[5] Si queremos triunfar en el dominio del ciberespacio, no podemos apoyarnos únicamente en la lógica "síentonces" y soluciones de ingeniería. Tenemos que maniobrar en el ciberespacio, pero para hacerlo de manera efectiva, es necesario comenzar por desarrollar a nuestra gente.

La creación de un cuadro competente de operadores del ciberespacio es una de mis primeras prioridades. Estamos trabajando arduamente para identificar los conjuntos de destrezas necesarios y determinar cómo desarrollar mejor el campo profesional. Sin embargo, el cambio debe trascender de los operadores del ciberespacio. Todos los elementos de la fuerza total deben aprender a pensar en el ciberespacio como un dominio de lucha de guerra, y que la garantía de misión no es algo que solo crean los expertos técnicos. El Aerotécnico que conecta un aparato no autorizado a una red o elude un control de seguridad en un cargador de mantenimiento debe entender que está creando vulnerabilidades que nuestros enemigos pueden explotar. Nuestros adversarios podrían implantar armas y anular nuestra capacidad de lograr nuestras misiones y, en última instancia, causar la muerte de valientes estadounidenses en el combate. Todo está conectado, y ese enlace cuestionable de correo electrónico puede permitir que un arma penetre los sistemas de misión. El hecho de que algunos de nuestros sistemas no utilicen sistemas operativos comerciales, como Windows, no es defensa contra un adversario

competente y con abundantes recursos. También debemos cambiar nuestro modo de pensar de tratar de impedir todo ataque hacia un enfoque de combatir los ataques y al mismo tiempo lograr nuestras misiones.

La capacidad de recuperación del ciberespacio será vital para el vuelo, la lucha y la victoria en un entorno ciberespacial disputado. Por lo tanto, los operadores del ciberespacio deberán ir más allá de la pregunta, "¿Cómo puedo asegurar mejor este sistema contra los ataques?" a esta otra "¿Cómo debo operar en un entorno cibernético disputado donde el enemigo podrá atravesar cuando menos algunas de mis defensas?" Esto requiere un cambio importante en el modo de pensar de los operadores del ciberespacio militar, incluyendo centrarse en las capacidades de respuesta, como planes y equipos de emergencia y respuesta en caso de incidentes.[6] Una de las mejores formas de lograr este cambio es mediante la formación agresiva y completa de "equipos rojos". Un equipo rojo es un grupo de atacantes amigables que intentan atacar sistemas para descubrir sus vulnerabilidades y debilidades. Utilizan las mismas técnicas que los atacantes del mundo real y proporcionan un invaluable servicio que detecta no solo vulnerabilidades sino que también ofrece a los defensores práctica en cómo reconocer y responder a los ataques para mantener sus sistemas funcionando. Los equipos rojos son vitales en ejercicios de gran escala que no son planificados y preparan a los defensores para hacer frente a adversarios que maniobran en alto nivel. El cambio a una defensa que se centra en capacidad de recuperación involucra un cambio de paradigma que es difícil para gran parte del personal militar. Antoine Bousquet ha resaltado la tendencia de los militares estadounidenses de buscar "'100% de contenido pertinente, 100% de precisión, y tiempo de retraso nulo', lo que permitirá el funcionamiento perfecto de una máquina de guerra cibernética sin fricción".[7] Por su parte el principio de capacidad de recuperación preconiza aceptar la incertidumbre y diseñar para la capacidad de adaptarse al fallo y lo imprevisto. La supuesta revolución en asuntos militares que iba a disipar la "niebla" de Clausewitz mediante información perfecta ha sido desacreditada en gran medida, pero aún resuena en las preferencias culturales de los militares estadounidenses de buscar la información perfecta. Los guerreros del ciberespacio no son los únicos que se deben adaptar; los operadores y el personal de apoyo centrados en los dominios físicos también deben practicar la operación efectiva en un entorno que constantemente está cambiando y donde no todo funciona como se espera. Aunque para los defensores esta capacitación es la más fácil de obtener en escenarios de ejercicios difíciles, algunas veces nos apartamos de tales escenarios debido al temor cultural de fracasar. ¿Cuál fue la última vez que una unidad militar estadounidenses luchó un ejercicio de "guerra" sin ninguna de sus computadoras funcionando? Con demasiada frecuencia el equipo rojo está atado de manos para evitar el cumplimiento de los objetivos del ejercicio. Sin embargo, aún no ha habido una guerra en la que el enemigo haya seguido el guión y haya hecho lo que se esperaba. Por lo tanto, debemos practicar tal como creemos que será la lucha en un entorno volátil, incierto, complejo y ambiguo. De aquí que un campo de batalla realista que represente con precisión los entornos del futuro sea esencial para que los combatientes se preparen para el fallo y para continuar luchando, incluso si temporalmente no cuentan con algunos de sus sistemas de lucha de guerra.

Bajo la dirección del Jefe de Estado Mayor de la USAF, convoqué a la Task Force Cyber Secure (Fuerza de tareas de seguridad del ciberespacio) para garantizar las cinco misiones fundamentales y mantener nuestra efectividad en la era de la información. La fuerza de tareas agrupó operadores del ciberespacio con miembros de nuestros equipos de operaciones e inteligencia para integrar esfuerzos a través de la Fuerza Aérea y concentrarse en pasos concretos para aprovechar las oportunidades y mantener nuestros riesgos dentro del ciberespacio. La fuerza de tareas ayudó a diagnosticar el problema, inició un diálogo interdisciplinario absolutamente esencial, y buscó medios para fomentar la educación y la cultura en el ciberespacio en toda la Fuerza Aérea. Por otra parte, la fuerza de tareas está creando una estructura duradera para que continúe el avance logrado, que incluye un oficial de seguridad jefe de información de la Fuerza Aérea, cambios en administración y financiación, y un foco perdurable de garantía de misión en el ciberespacio. No podemos darnos el lujo de esperar mientras nuestros adversarios mejoran su capacidad de poner en peli-

gro nuestras misiones fundamentales, y será necesario que todos los que formamos parte de la fuerza total aseguremos nuestra posición de primera fuerza aérea del mundo en la era de la información. ❑

Notas

1. Publicación conjunta 3-13, *Information Operations (Operaciones de información)*, 27 de noviembre de 2012 (que incorpora el cambio 1, del 20 de noviembre de 2014), II-9, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
2. Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower (Un enfoque ambiental para entender el ciberpoderío)", en *Cyberpower and National Security (Ciberpoderío y Seguridad Nacional)*, ed. Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (Washington, DC: Potomac Books, 2009), 256.
3. Gregory J. Rattray, *Strategic Warfare in Cyberspace (La guerra estratégica en el ciberespacio)* (Cambridge, MA: MIT Press, 2001), 18–19.
4. Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World (La guerra cibernética: Cómo los conflictos en el ciberespacio desafían a los Estados Unidos y cambian el mundo)* (Santa Barbara, CA: Praeger, 2013), 20.
5. Carl von Clausewitz, *On War (Sobre la Guerra)*, editado y traducido por Michael Howard y Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.
6. Rattray, *Strategic Warfare in Cyberspace* (Guerra estratégica en el ciberespacio), 209.
7. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity (El modo científico de la guerra: Orden y caos en los campos de batalla de la modernidad)* (New York: Columbia University Press, 2009), 222.

Teniente General William J. Bender, USAF (BE, Manhattan College; MA, Embry-Riddle Aeronautical University; MA, US Army War College), es el jefe de la Oficina del Dominio de Sistemas de Información y Oficial en Jefe de Información, Oficina del Secretario de la Fuerza Aérea, Pentágono, Washington DC. El General Bender está a cargo de tres direcciones y apoya 54.000 operaciones cibernéticas y personal de apoyo a lo largo del mundo con una cartera valorada en US$17 mil millones. El General Bender tiene la responsabilidad general de la cartera de tecnología de información en calidad de autoridad superior para la estrategia de inversión de la tecnología de información, redes, directrices centradas en la red, comunicaciones, gestión de recursos de información, seguridad de la información y otros asuntos afines para el Departamento de la Fuerza Aérea. En calidad de oficial jefe de información, el General Bender supervisa la administración de la cartera, suministra arquitectura empresarial y hace cumplir las leyes de la Ley de Libertad de Información y la Ley de Privacidad. El General Bender integra las capacidades bélicas y de apoyo de la misión interconectando los recursos aéreos, espaciales y terrestres. Además, desarrolla la doctrina, estrategia y directriz para todas las operaciones ciberespaciales y las actividades de apoyo.

Coronel William D. Bryant, USAF (USAFA; MA, American Military University; MA, George Washington University; MSS [Maestría en Sistemas Espaciales], Air Force Institute of Technology; MAAS [Maestría en el Arte y la Ciencia del Poderío Aéreo]; PhD, School of Advanced Air and Space Studies; MSS [Maestría en Estudios Estratégicos], Air War College) es subdirector de la Fuerza de Tarea de Seguridad Cibernética para la Oficina del Dominio de la Información y del Oficial en Jefe de Información, Oficina del Secretario de la Fuerza Aérea, Pentágono, Washington DC. El Coronel Bryan es un piloto de combate de carrera y un estratega, que ha servido en numerosas asignaciones operacionales y de estado mayor..