Encaminándonos hacia el Éxito en la Misión Cibernética de la Fuerza Aérea

Aprovechándonos de nuestro legado para forjar nuestro futuro

Teniente General David S. Fadok, USAF
Dr. Richard A. Raines

HACE TAN SOLO unas décadas, considerábamos que el poderío aéreo era principalmente tripulaciones calificadas piloteando aeronaves de combate y lanzando bombas sobre blancos. Hoy significa mucho más. Por ejemplo, 16 de los 18 hombres del aire cuyos logros heroicos se destacan en la última edición de Portraits in Courage del Jefe de Estado Mayor de la Fuerza Aérea no son aviadores y 15 son personal alistado.[1] Sin embargo, todos ellos suministraron poderío aéreo en las líneas del frente de combate, ya sea conduciendo convoyes, deshaciéndose de pertrechos explosivos, ofreciendo seguridad fuera de los cuarteles, desempeñándose como instructores de las fuerzas afganas e iraquíes u ordenando ataques de precisión desde aeronaves en vuelo. De hecho, en la versión más reciente de nuestro documento de doctrina culminante, AFDD 1, Air Force Basic Doctrine, Organization, and Command (Doctrina básica, organización y mando de la Fuerza Aérea), se reconoce esta naturaleza cambiante del poderío aéreo al definirlo como "la capacidad de proyectar poder militar o influencia a través del control y utilización del aire, espacio y ciberespacio para lograr objetivos estratégicos, operacionales y tácticos".[2]

El General de Fuerza Aérea, Henry "Hap" Arnold, ofreció asesoramiento sabio cuando expresó que "debemos pensar en términos del mañana".[3] Gran parte del poderío aéreo del mañana tendrá lugar en el ámbito operacional emergente del ciberespacio. El adelanto rápido en las tecnologías de computadoras y comunicaciones, al igual que el vínculo estrecho del "ámbito digital" con las operaciones físicas, hacen que el ciberespacio sea cada vez más importante para el éxito militar. Los retos planteados por el ciberespacio reflejan su naturaleza global, las soberanías políticas que trasciende y el hecho de que las operaciones ocurren a la velocidad de la luz. Estados Unidos, por mucha imaginación que pongamos, no puede disfrutar en el ciberespacio la ventaja clara y asimétrica que disfrutamos en los ámbitos de la tierra, mar, aire y espacio.

Por medio de correos electrónicos, sitios web sociales y otras formas de comunicación electrónica compartimos información instantáneamente a lo largo de la red informática mundial. A pesar de que esta capacidad ha disminuido sustancialmente, el tiempo necesario para tomar decisiones ha aumentado nuestra dependencia en los sistemas de comunicación. La información a través del ciberespacio a velocidades extremadamente rápidas y, a diferencia de los ataques cinéticos tradicionales, los ataques ciberespaciales pueden comenzar, detenerse y cambiar completamente en cuestión de segundos…sin avisar. Por consiguiente, nuestros hombres del aire deben estar preparados para reaccionar de inmediato—y aquí radica el reto.

Las proverbiales "computadora portátil y conexión a la Internet" proveen una entrada a un costo extremadamente bajo al juego de la explotación del ciberespacio. Como resultado, el adversario ciberespacial moderno es, y continuará siendo, sumamente ágil e innovador. Nos esforzamos por crear pautas y políticas para operaciones ciberespaciales rápidas y precisas, pero los adversarios han resultado ser expertos en crear métodos nuevos y creativos para explotar y atacar el ciberespacio, muchas veces utilizando contra nosotros las restricciones de nuestro propio sistema jurídico. El entorno cibernético cambia tan rápidamente que alguien puede alegar que puede que nuestras directrices sean obsoletas cuando finalmente se aprueben. Además, enfrentamos el verdadero peligro de que no podemos elaborar doctrina y tácticas lo suficientemente rápido como para seguir el ritmo de las amenazas operacionales cambiantes en el ciberespacio.

Por años, el ciberespionaje y la explotación han existido a una escala global. No limitadas a las naciones estados, estas acciones también han involucrado actores de la industria, el crimen organizado, grupos activistas y terroristas. Obviamente, los motivos varían según el grupo, pero en la mayoría de los casos, el ciberespionaje y la explotación son impulsados por ganancias en finanzas y la propiedad intelectual. En la Fuerza Aérea estamos preocupados por proteger nuestros recursos críticos y la propiedad intelectual al igual que perseguir blancos mediante medios cibernéticos según lo permiten el Código de Estados Unidos y las autoridades competentes. Para ello, debemos crear los líderes de pensamiento, la fuerza laboral cibernética, conceptos operacionales y las capacidades tecnológicas para poder ejecutar con éxito durante tiempos de conflictos cibernéticos o ciberguerra.

En los debates en curso se trata lo que constituye la ciberguerra y si estamos o no en guerra en el ciberespacio. En este artículo no se tratan esos temas; en cambio, se sugiere cómo la Fuerza Aérea y la Universidad del Aire deben seguir adelante para estar al frente y apoyar las necesidades de seguridad cibernética de nuestra nación. Por lo tanto, se enfoca en lecciones análogas aprendidas de la historia, nuestra postura en la actualidad y lo que necesita ser, y los planes para llegar ahí con respecto a nuestras capacidades ciberespaciales.

Nuestro legado: La escuela táctica del cuerpo aéreo

Durante los años entre la Primera y la Segunda Guerra Mundial, grandes pensadores se reunieron en la Escuela Táctica del Cuerpo Aéreo (ACTS, por sus siglas en inglés), la progenitora de la Universidad del Aire. ACTS reunió algunas de las personas más inteligentes disponibles

para definir, crear y demostrar la mejor manera para controlar y explotar el ámbito nuevo del espacio aéreo. Estos aviadores pioneros emplearon sus talentos colectivos para impulsar el desarrollo de tecnologías necesarias para implementar las capacidades de poderío aéreo. Desde los pizarrones en los salones de clase hasta la práctica en los cielos, ACTS ofrecía un entorno de aprendizaje para el desarrollo inicial del poderío aéreo y un campo de prueba para el perfeccionamiento de los conceptos y tecnologías propuestas. Los estudiantes se convirtieron en instructores y viceversa, compartiendo ideas y conceptos por casi 20 años. Al promover el pensamiento de poderío aéreo, ellos ejercieron una gran influencia sobre cómo condujimos las operaciones aéreas durante la Segunda Guerra Mundial.

Uno de esos grandes pensadores, el General Muir Fairchild, se convertiría en el primer comandante de la Universidad del Aire. Cuando sus puertas abrieron en 1946, él decidió que esta nueva institución adoptaría el lema "ACTS: Proficimus More Irretenti (Progresamos sin ser obstaculizados por las costumbres). Desde los inicios de ACTS, la Fuerza Aérea ha continuado como líder del adelanto de los conceptos y capacidades del poderío aéreo mediante métodos nuevos e innovadores para mejorar nuestra eficacia en el ámbito aéreo. Estos éxitos podemos atribuirlos en gran parte a los talentosos e ingeniosos aviadores, hombres y mujeres, que encontraron soluciones a los problemas.

Solucionando los retos cibernéticos de hoy para la fuerza aérea del mañana

Mucho ha cambiado desde que ACTS estableció las bases del poderío aéreo. Ahora nos encontramos en un entorno global, de acceso instantáneo a la información donde el conflicto puede comenzar en un abrir y cerrar de ojos sin pruebas aparentes. El ciberespacio ha creado un ámbito en el que el conflicto puede pasar desapercibido y sin atribuciones. Como se mencionó anteriormente, el ámbito ciberespacial admite jugadores a un precio bajo de entrada, muchos de ellos sumamente capacitados y hábiles. En vista de la rapidez de los eventos ciberespaciales, la protección y el control de la información para garantizar el éxito de nuestra misión son de suma importancia. La exfiltración de información de nuestros recursos cibernéticos, al igual que ataques a nuestros recursos críticos, exige que desarrollemos rápidamente los medios para contrarrestar esas acciones adversarias y que a la vez elaboremos y maduremos nuestras capacidades en las operaciones cibernéticas de ofensiva. La Fuerza Aérea y el Departamento de Defensa (DoD, por sus siglas en inglés) deben contar con el liderazgo y una fuerza laboral capaz de comprender cómo el ciberespacio se puede y se usará contra nosotros, y cómo lo podemos utilizar para entregar opciones soberanas a nuestros líderes políticos nacionales. Debemos avanzar, crear, comprobar y desplazar esas opciones a nuestros guerreros. La educación, adiestramiento, investigación, pruebas, evaluación y desarrollo deben recalcar la seguridad de la misión, indistintamente del ámbito en el que se opera.

Actualmente, el ciberespacio de la Fuerza Aérea debe tomar en cuenta dos tareas: crear y sostener una fuerza laboral para cumplir con los problemas del mañana, y crear conceptos y capacidades para contrarrestar al igual que mitigar los esfuerzos de nuestros adversarios expertos. La primera tarea resultara difícil, impulsada principalmente por presupuestos de defensa reducidos y compromisos con nuestras áreas de misión básicas.

Las operaciones ciberespaciales continuarán retándonos con incógnitas y amenazas que surgen rápidamente de complejidades cada vez mayores. La excelencia cibernética debe basarse en la educación e investigación cibernética superior. Las operaciones a la velocidad de la luz exigen un desarrollo rápido y eficaz y el empleo de conceptos operacionales y capacidades tecnológicas para ayudar a disminuir las demandas en el guerrero/operador cibernético. Los conceptos y las

capacidades deben cumplir con las necesidades de la misión del comandante y garantizar operaciones eficaces con un nivel de certeza sumamente elevado.

El camino a seguir: La escuela táctica del cuerpo aéreo ciberespacial

Últimamente, hemos escuchado varias referencias a la noción de que, en términos ciberespaciales, nos encontramos nuevamente en los años entre las guerras. Si esto es cierto, quizás es hora de establecer una ACTS "Cibernética" (C-ACTS, por sus siglas en inglés), donde podamos reunir pensadores estratégicos importantes de todos los participantes principales en el gobierno (tanto dentro como fuera de la Universidad del Aire) y del sector privado con el propósito de identificar ideas en nuestro ámbito más nuevo del ciberespacio. Una C-ACTS exitosa lograría lo siguiente:

- Enlazaría y se aprovecharía de talentos y recursos de la educación, ciencia y tecnología, al igual que de las comunidades operacionales.
- Albergar e interactuar de cerca con innovadores de las comunidades mencionadas anteriormente quienes poseen credenciales excelentes en el mundo académico, investigación y desarrollo y experiencia.
- Ofrecer un foro para la creatividad, innovación e intercambio, no solo para cultivar ideas sino también para crear y probar rápidamente los prototipos y poner en funcionamiento los sistemas.
- Unir fuertemente las innovaciones y el desarrollo tecnológico con la evolución de las tácticas y doctrina.
- Mezclar la educación moderna con el aprendizaje interactivo (o sea, "echar a volar" las ideas cibernéticas).
- Integrar estrechamente los desarrollos cibernéticos en los requerimientos generales de la seguridad de la misión para ofrecer cursos de acción no cinéticos eficaces al encargado de tomar decisiones.

En vista de que vivimos y operamos en un entorno descentralizado, no debemos alojar una C-ACTS exclusivamente dentro de la estructura de una sola organización. Contamos con muchas organizaciones duchas en cibernética que podemos y debemos aprovechar. A nivel nacional, la Agencia Central de Inteligencia, DOD, Departamento de Energía, Departamento de Seguridad Interna y la Agencia Federal de Investigación poseen operaciones cibernéticas intrínsecas y capacidades de desarrollo con responsabilidades cibernéticas singulares pero que a veces coinciden. Dentro del DOD, el Comando Cibernético de EE.UU., la Agencia de Seguridad Nacional y cada uno de los servicios armados cuentan con operaciones cibernéticas decretadas para llevar a cabo operaciones bajo la autoridad de los Títulos 10, 18, 32 y 50. Las academias de los servicios del DOD pueden ofrecer educación cibernética básica, mientras que en instituciones tales como el Instituto de Tecnología de la Fuerza Aérea y la Escuela de Posgrado de la Armada ofrecen educación cibernética continua, avanzada y a nivel de posgrado. La Fuerza Aérea y la Armada ostentan poseer extensas capacidades a través de sus Comandos de Educación y Adiestramiento de la Fuerza Aérea y las Fuerzas Cibernéticas, respectivamente. El Ejército y el Cuerpo de Infantería de Marina se aprovechan de las capacidades existentes de educación y adiestramiento de los servicios hermanos a la vez que crean capacidades específicas a la misión mediante sus propios Comandos Cibernéticos. Además, las capacidades de investigación y desarrollo radican en

los laboratorios de investigación de cada uno de los servicios armados. También la industria y el ámbito académico desempeñan papeles importantes en el desarrollo del capital cibernético tanto humano como tecnológico.

La Universidad del Aire está avanzando con el concepto C-ACTS para crear un entorno mejor para compartir información y fomentar ideas. Basándonos en asociaciones existentes y creando nuevas según sea apropiado, buscamos colaborar de cerca con nuestros socios operacionales en la Vigésima Cuarta Fuerza Aérea y nuestros socios de investigación y desarrollo en el Laboratorio de Investigaciones de la Fuerza Aérea para garantizar el rendimiento de la inversión en actividades cibernéticas. A lo largo de la Universidad del Aire, contamos con recursos que apoyan la C-ACTS. El Centro para Investigaciones Cibernéticas, designado como el Centro de Excelencia Técnico Ciberespacial de la Fuerza Aérea y ubicado en el Instituto de Tecnología de la Fuerza Aérea, está encargado de coordinar los esfuerzos C-ACTS. Esta tarea complementa aquellas emitidas en el 2008 por el Secretario de la Fuerza Aérea para que el Centro de Investigaciones Ciberespaciales "estableciera los vínculos" con respecto a quién hace qué en la educación, investigación y desarrollo ciberespacial.

Reflexiones finales

La Fuerza Aérea está llevando a cabo operaciones durante un tiempo de cambio dinámico. Las operaciones en y a través del ciberespacio exigirán tácticas, técnicas y procedimientos nuevos al igual que mentalidades de liderazgo nuevo para contrarrestar las acciones del enemigo. Debemos crear rápidamente y mantener la siguiente generación de líderes y guerreros cibernéticos que enfrentarán una era de información compleja y el ámbito ciberespacial de las operaciones. Nosotros en la Universidad del Aire enfrentaremos el reto de crear y dotar a nuestros líderes y guerreros cibernéticos con el conocimiento y la experiencia que necesitan para garantizar la misión y el éxito operacional. Tal como el General Arnold aconsejó, continuaremos pensando en términos del mañana, buscando un progreso sin ser obstaculizados por las costumbres en el ámbito operacional más nuevo del ciberespacio. ❑

Notas

1. Department of the Air Force, Portraits in Courage: Airmen in the Fight, vol. 6 (Washington, DC: Department of the Air Force, 2011), http://www.af.mil/shared/media/document/AFD-110921-035.pdf.

2. Air Force Doctrine Document 1, Air Force Basic Doctrine, Organization, and Command, 14 de octubre de 2011, 11, http://www.e-publishing.af.mil/shared/media/epubs/afdd1.pdf.

3. H. H. Arnold, Global Mission (Misión global) (New York: Harper, 1949), 615.

El Teniente General David S. Fadok, USAF (USAFA; MA, Oxford University; MAAS, School of Advanced Airpower Studies, Air University) es comandante y presidente de la Universidad del Aire, Base Aérea Maxwell, Alabama. Él ofrece el espectro completo de educación, investigación y divulgación en cada nivel mediante la educación militar profesional, la educación continua profesional y el otorgamiento de títulos académicos. El General está al frente del centro intelectual y de liderazgo de la Fuerza Aérea de EE.UU., de donde anualmente egresan más de 50.000 oficiales residentes y 120.000 oficiales no residentes, al igual que personal alistado y civil. Además, el General es responsable del nombramiento de oficiales mediante la Escuela de Capacitación para Oficiales y el Cuerpo de Adiestramiento de Oficiales de la Reserva. Anteriormente, se desempeñó en calidad de comandante del Centro Curtis E. LeMay para el Desarrollo de la Doctrina y la Educación y en calidad de Vicecomandante de la Universidad del Aire. El General Fadok culminó sus estudios de posgrado como becado de Rhodes antes de obtener sus alas de piloto en 1985. Un piloto comandante con más de 4.000 horas de vuelo, anteriormente se desempeñó en calidad de comandante a los niveles de escuadrón, grupo y ala. Voló en misiones de combate y de apoyo de combate en las operaciones Causa Justa, Escudo en el Desierto, Tormenta en el Desierto y Southern Watch. En calidad de egresado distinguido de la Escuela para Oficiales de Escuadrón y de la Escuela Superior de Comando y Estado Mayor de la Fuerza Aérea, al igual que Becado de la Defensa Nacional, en 1988 el General Fadok recibió el Premio de Liderazgo del Secretario de la Fuerza Aérea.

El Dr. Richard A. Raines (BSEE, Florida State University; MS, Air Force Institute of Technology; PhD, Virginia Tech) es el director del Centro de Investigaciones Ciberespaciales de la Fuerza Aérea, presidente de Transformación de la Fuerza del Departamento de Defensa y profesor de ingeniería eléctrica en el Instituto de Tecnología de la Fuerza Aérea, Base Aérea Wright-Patterson, Ohio. El Dr. Raines se desempeña en calidad de asesor técnico para numerosas organizaciones del gobierno de Estados Unidos y grupos de trabajo federales de seguridad cibernética. Ha escrito más de 150 publicaciones técnicas y estratégicas sobre comunicaciones y ciberseguridad. En el 2007 fue iniciado en la Asociación Old Crows' Hall of Fame por sus aportes a las operaciones de información y en el 2008 recibió el premio del año al Educador de Ciencia y Energía de la Fuerza Aérea. El Dr. Raines es miembro principal del Instituto de Ingenieros Electricistas y Electrónicos.