La Conducción de la Guerra en el Ciberespacio

Desarrollando la Presentación de la Fuerza y el Mando y Control

Teniente Coronel (USAF) M. Bodine Birdwell
Teniente Coronel (USAF-Ret.) Robert Mills, PhD

EL DEPARTAMENTO DE Defensa (DOD) se está esforzando por definir la conducción de la guerra en el ámbito del ciberespacio global.[1] La creación del Comando Ciberespacial de EE.UU. (USCYBERCOM), un comando combatiente funcional subunificado (FCC, por sus siglas en inglés) bajo el Comando Estratégico de EE.UU. (USSTRATCOM), es un paso enorme en integrar y coordinar la defensa, protección y funcionamiento de las redes del DOD. Sin embargo, este paso no significa que el USCYBERCOM llevará a cabo o administrará todas las misiones ciberespaciales. De hecho, la gran mayoría de las misiones ciberespaciales llevadas a cabo por los servicios armados y los comandos combatientes (COCOM, por sus siglas en inglés), aunque vitales para mantener el acceso al ámbito en apoyo a sus operaciones, no son de una naturaleza bélica *activa*. Aplicamos los conceptos clausewitzianos de conducción de la guerra, ofensiva y defensa activa al ámbito ciberespacial y proponemos varias recomendaciones para ayudar al USCYBERCOM a medida que colabora con los servicios armados y los comandos geográficos combatientes (GCC, por sus siglas en inglés) para luchar en el ciberespacio. El hecho de que los comandantes globales, regionales y de los servicios armados tendrán que compartir el mando y control (C2) de las capacidades bélicas y las fuerzas del ciberespacio suscita varias preguntas interesantes acerca de cómo el USCYBERCOM puede colaborar de la manera más eficaz con los GCCs. Específicamente, ¿cuál es el método ideal para la presentación de las fuerzas, y qué modelo de C2 debe emplear el DOD para las capacidades bélicas en el ciberespacio? ¿Hay lecciones aprendidas de retos de apoyo global a regional similares que pudiésemos aplicar al C2 ciberespacial? Ofrecemos el Comando de Operaciones Especiales de EE.UU. (USSOCOM, por sus siglas en inglés) como un modelo para la presentación de la fuerza ciberespacial y el C2; sin embargo, ese modelo es una meta a largo plazo que no se puede lograr inmediatamente. Entretanto, el USCYBERCOM puede adaptar lecciones aprendidas de la presentación de fuerzas espaciales y de movilidad aérea y C2 para crear un método modular para evolucionar la presentación de la fuerza cibernética y el C2 de su estado naciente actual a un estado más maduro estilo USSOCOM.

Aunque hay otros modelos, examinamos cómo los modelos de la presentación de las fuerzas espaciales, de movilidad aérea y de operaciones especiales y el C2 pueden informar la manera como el USCYBERCOM pudiese interactuar con otros COCOMs, particularmente los GCCs. Además, tratamos las interdependencias complejas, las capacidades especializadas y los métodos doctrinales que los FCC utilizan a medida que les proporcionan sus capacidades a los GCCs. Para comenzar, tratamos brevemente lo inadecuado de la doctrina actual para la conducción de la guerra en el ciberespacio. Luego analizamos cómo la doctrina espacial y de movilidad aérea pueden ser modelos útiles, aunque adecuados solamente en parte, para presentar las

fuerzas y llevar a cabo C2. Por último, proveemos una metodología estandarizada que nos lleva de las capacidades actuales a un modelo ciberespacial completamentea desarrollado estilo USSOCOM.

Por qué el modelo existente de operaciones de información es insuficiente

La doctrina actual conjunta y de la Fuerza Aérea que rige la conducción de la guerra en el ciberespacio es escasa. Según el *Air Force Doctrine Document* (Documento de Doctrina de la Fuerza Aérea) (AFDD, por sus siglas en inglés) 3-12, *Cyberspace Operations* (Operaciones Ciberespaciales), "Aunque las operaciones ciberespaciales son esenciales para todos los comandos combatientes, los servicios armados y las fronteras de agencias, hasta la fecha de publicación de este AFDD, no hay una doctrina conjunta global para la planificación o las operaciones en el ciberespacio".[2] Se está coordinando oficialmente una nueva publicación de la doctrina ciberespacial conjunta, pero la doctrina conjunta publicada, al igual que una discusión de las operaciones de la red de computadoras como subconjunto de las operaciones de información (IO, por sus siglas en inglés), ni siquiera se aproxima al tema de la conducción de la guerra en el ciberespacio.[3] Las operaciones de la red de computadoras y las IO obviamente están relacionadas, pero sus finalidades son distintas. El General Keith B. Alexander, comandante del USCYBERCOM, escribió lo siguiente: "Aunque se entiende que la guerra terrestre, marítima, aérea y espacial se empleará para disuadir (por ejemplo, influenciar) a un adversario, nadie cree que la guerra dentro de esos ámbitos es solamente 'operaciones de información'".[4]

Tanto en el AFDD 3-12 y el General Alexander reconocen que la conducción de la guerra en el ciberespacio es algo más que un subconjunto de IO; sin embargo, en este momento la Joint Publication (JP) (Publicación Conjunta [JP, por sus siglas en inglés]) 3-13, *Information Operations I* (Operaciones de Información I), ofrece el único marco que trata el C2 para la conducción de la guerra en el ciberespacio. La doctrina conjunta no contiene ninguna orientación sobre la presentación de fuerzas ciberespaciales. En la doctrina de IO se definen las operaciones en la red de computadoras, que comprenden el ataque a redes de computadoras (CAN, por sus siglas en inglés), la defensa de redes de computadoras (CND, por sus siglas en inglés), y el aprovechamiento de la red de computadoras.[5] Para fines de este artículo, definimos los actos de guerra cibernética como CNA, además de un subconjunto de CND, conocido como acciones en respuesta a la CND (CND-RA, por sus siglas en inglés).[6] Según el JP 3-13, las actividades de CNA ahora están integradas al nivel de teatro en la célula J-39 de IO.[7] En el JP 6-0, *Joint Communications System* (Sistema Conjunto de Comunicaciones) se destaca que la CND está integrada dentro del J-6.[8] Este arreglo es problemático porque divide las funciones relacionadas con la conducción de la guerra entre diferentes elementos de estado mayor y esencialmente minimiza la importancia de un ámbito para la conducción de la guerra enterrándolo dentro del Estado Mayor Conjunto.

La doctrina conjunta debe separar la responsabilidad compartida de mantener acceso al ámbito ciberespacial, que debe ser una misión del J-6 (communicaciones), del concepto de la conducción de la guerra en el ciberespacio, que debe ser una misión del J-3 (operaciones).[9] El General Alexander destacó que, "Si bien el efecto principal de las IO es influenciar a un adversario a que *no* tome una acción, el efecto principal de la ciberguerra es negarle al enemigo la libertad de acción en el ciberespacio", (énfasis en el original).[10] A fin the participar en una ciberguerra como el General Alexander la imagina, la responsabilidad de CAN y CND-RA debe ampliarse más allá del Estado Mayor Conjunto y se debe tratar igual que la guerra en otros ámbitos.

Definiendo la presentación de las fuerzas

La presentación de las fuerzas para la ciberguerra es la manera como el USCYBERCOM y los servicios armados ponen a disposición de los GCCs las capacidades de CNA y de CND-RA. En el JP 1, *Doctrine for the Armed Forces of the United States* (Doctrina para las Fuerzas Armadas de Estados Unidos), se hace un resumen de los roles y responsabilidades de los servicios armados y de los COCOMs:

> Los servicios armados y el Comando de Operaciones Especiales de Estados Unidos (en zonas exclusivamente dedicadas a las operaciones especiales) tienen las responsabilidades de organizar, adiestrar, equipar y sostener fuerzas. . . .
>
> Los Comandantes del Comando Central de EE.UU., del Comando de EE.UU. en Europa, del Comando de EE.UU. en el Pacífico, del Comando Sur de EE.UU. y del Comando Norte de EE.UU. . . . (1) impiden ataques contra Estados Unidos, sus territorios, posesiones y bases, y emplean la fuerza apropriada en caso de que fracase la disuasión; (2) llevan a cabo misiones y tareas asignadas y planifican y ejecutan operaciones militares, según se les ordena, en apoyo a las pautas estratégicas.[11]

En calidad de componentes del DOD encargados de librar guerras, los COCOMs definen los requisitos, y los servicios armados organizan, adiestran, equipan y sostienen las fuerzas para cumplir con esos requisitos. En la actualidad, el USSOCOM es singular porque es un COCOM con responsabilidades parecidas a las de un servicio.

La presentación de fuerzas y los modelos de C2 para las operaciones espaciales, de movilidad aérea y de fuerzas especiales forman pasos a lo largo de una continuidad de opciones que el USCYBERCOM puede usar cuando provea fuerzas bélicas y capacidades a los GCCs. El primer paso, presentación de la fuerza espacial, se basa en un modelo de acción independiente que el USSTRATCOM emplea para controlar la presentación de la fuerza espacial y apoyar a los GCCs. El segundo paso, presentación de la fuerza de movilidad aérea, se basa en un modelo de acción interdependiente mediante el cual el Comando de Transporte de EE.UU. (USTRANSCOM) colabora con los GCCs para trasladar fuerzas y abastos en todo el mundo. Por ultimo, la presentación de fuerzas de la fuerzas de operaciones especiales (SOF, por sus siglas en inglés) se basa en un modelo orgánico de presentación de fuerzas.

Primer Paso: Un modelo espacial—acción independiente

En la actualidad, a medida que el DOD desarrolla capacidades bélicas cibernéticas, no contamos con suficientes guerreros de ciberguerra disponibles para distribuirlos de manera descentralizada entre los GCCs. Emplear un modelo de acción independiente le permitiría al USCYBERCOM apoyar la cifra máxima de requerimientos GCC porque el USCYBERCOM podría cambiar dinámicamente sus recursos limitados para maximizar el apoyo al GCC. Durante décadas, USSTRATCOM ha hecho esto con la presentación de la fuerza espacial. Aplicar conceptos de la doctrina espacial podría ayudar al USCYBERCOM a tomar medidas inmediatas para mejorar la presentación de la fuerza cibernética a los GCCs.

El General Kevin P. Chilton, comandante del USSTRATCOM, claramente conectó el espacio al ciberespacio: "Pasemos a la línea de operación que llamamos el ciberespacio. ¿Acaso esa es una línea de apoyo para nosotros? ¡Seguro! Al igual que el espacio. ¿Acaso es global por naturaleza? ¡Seguro! Al igual que el espacio. ¿Operamos en ella todos los días? ¡Seguro! Al igual que el espacio. De hecho, lo que se nos exige que hagamos es operar, defender, prepararnos para atacar y atacar a través de este ámbito al recibir la orden".[12]

Las acciones del USSTRATCOM en el espacio ocurren independientemente de cualesquier medidas que se tomen en el teatro. Ese comando no depende del GCC para llevar a cabo alguna tarea antes que pueda completar sus tareas en el espacio. No obstante, la relación espacial es una intrísecamente dependiente de la perspectiva del GCC. Por este motivo, los GCC deben informarle explícitamente al USSTRATCOM todos los requerimientos

de apoyo espacial; hacer lo contrario posiblemente interrumpiría o afectaría de manera negativa las operaciones bélicas del GSS que dependen del apoyo espacial.

La presentación de las fuerzas espaciales y la plantilla del C2 centralizan todas las comunicaciones del GCC a través de un canal especificado dentro del USSTRATCOM conocido como el comando conjunto del componente funcional espacial (JFCC Space, por sus siglas en inglés). Ese canal se comunica con todos los GCCs y mantiene la información de la situación de cómo las operaciones espaciales se integran con todas las activiades del GCC. Para poderse comunicar eficazmente, el JFCC Space utiliza el centro conjunto de operaciones espaciales (que se basa en el concepto de un centro de operaciones aéreas y espaciales [AOC], por sus siglas en inglés]) para mandar y controlar eficazmente las operaciones espaciales militares.

USSTRATCOM ha delegado las actividades diarias de las comunicaciones al JFCC Space. Asimismo, en el JP 3-14, *Space Operations* (Operaciones Espaciales), se destaca que "[los comandantes del GCC] pueden designar una autoridad coordinadora espacial (SCA, por sus siglas en inglés) y delegar autoridades apropiadas para planificar, integrar y coordinar las operaciones espaciales dentro de la zona operacional".[13] En muchos aspectos, la SCA sirve como el punto central del COCOM para todas las operaciones de apoyo espacial. Una SCA puede trabajar con JFCC Space para todo tipo de asuntos de apoyo espacial. El concepto de la SCA sirve como un modelo entre ámbitos para las comunicaciones entre el USSTRATCOM y el GCC. La SCA recopila los requerimientos de todos los componentes del servicio armado y funcional y, en nombre del GCC, se comunica al unísono con USSTRATCOM vía JFCC Space.

Logrando la acción independiente del USCYBERCOM: Autoridad Coordinadora Cibernética. Con el fin de aumentar la visibilidad de las actividades de guerra cibernética, cada GCC debe adoptar el concepto SCA para la presentación de la fuerza cibernética, de hecho crear una autoridad coordinadora cibernética (CCA, por sus siglas en inglés). Esta acción es viable hoy en día porque requiere recursos limitados. El mayor reto de crear un puesto CCA dentro de cada GCC radica en definir su ubicación adecuada. La doctrina espacial con respecto a la ubicación de la SCA le difiere esa decisión a cada GCC.[14] USCYBERCOM podría seguir la plantilla de la doctrina espacial de diferir la decisión a cada GCC, o podría recomendar la ubicación de una CCA para integrar mejor las actividades del USCYBERCOM dentro del esquema de maniobra del GCC.

Además, si se crease una CCA, USCYBERCOM podría continuar completando de manera centralizada muchas de sus funciones bélicas. Al igual que las operaciones espaciales, la relación permanecería independiente de la perspectiva del FCC y dependiente de la persepctiva del GCC. Dentro del GCC, los servicios armados mantienen y operan sus propias redes. USCYBERCOM dirigiría todas las actividades CAN y CND-RA en nombre del GCC.

La doctrina espacial ofrece conocimientos de la presentación de la fuerza ciberespacial más allá del nivel de cuartel general de la fuerza conjunta. USSTRATCOM dirige a sus componentes del servicio (en lo que respecta al espacio) para que sirvan en calidad de defensores del espacio dentro de su servicio armado, especialmente los componentes de servicios de los GCCs:

> Las responsabilidades comunes de cada uno de los componentes de los servicios armados son: abogar por los requerimientos espaciales dentro de sus respectivos servicios, proveer un solo punto de contacto para acceso a las capacidades y recursos de los servicios, hacer recomendaciones al USSTRATCOM con respecto al empleo apropiado de las fuerzas de los servicios, proveer fuerzas espaciales asignadas al CDRUSSTRATCOM (comandante, USSTRATCOM) y a los CCDRs (comandantes combatientes) según se les ordene, asistir en la planificación en apoyo a las operaciones espaciales y tareas asignadas, y apoyar al CDRUSSTRATCOM y otros CCDRs con conocimientos en el campo de las misiones espaciales y apoyar las capacidades deseadas según se les soliciten.[15]

USSTRATCOM le dispersa la pericia espacial que radica en sus componentes del servi-

cio a los componentes del servicio del GCC para proveerles a los GCCs "conocimientos y apoyo en el campo de las misiones espaciales", tal como se mencionó anteriormente. Este enfoque le permite al USSTRATCOM centralizar las capacidades de C2 espaciales a la vez que garantiza que los componentes GCC estén al tanto de las capacidades espaciales. Esos defensores del espacio ayudan a los componentes del GCC a integrar las capacidades espaciales dentro de sus operaciones.

Logrando la acción independiente del USCYBERCOM: Responsabilidades del Componente del Servicio. Los componentes del servicio del USCYBERCOM deben actuar en calidad de defensores de las CAN y CND-RA dentro de cada GCC. Esos componentes deben enviar enlaces para que aboguen por las capacidades bélicas cibernéticas dentro del servicio respectivo GCC y componentes funcionales para maximizar la contribución del USCYBERCOM a las actividades bélicas del GCC. La doctrina espacial provee una plantilla para integrar el espacio dentro de los componentes del servicio, empleando elementos de apoyo espacial del Ejército, los oficiales de operaciones espaciales de la Armada, el equipo espacial de la Infantería de Marina y el director de las fuerzas espaciales de la Fuerza Aérea.[16] Aunque el USSTRATCOM no cuenta con un componente de operaciones especiales, sí mantiene un concepto de equipo de apoyo espacial para enviar "defensores" del espacio a los componentes de operaciones especiales del GCC.[17] Los defensores fijos de la guerra cibernética abogarían por métodos mediantes los cuales las acciones CAN/CND-RA del USCYBERCOM podrían ayudar a cumplir los requerimientos del GCC, los cuales entonces le llegarían al USCYBERCOM via la CCA del GCC.

Segundo Paso: Un modelo de movilidad aérea—acción interdependiente

Crear una CCA y dispersar defensores en todo el GCC asentaría una base fuerte sobre la cual construir una metodología madura para la presentación de la fuerza cibernética. Esas medidas iniciales de aprovechar las lecciones aprendidas de la presentación de la fuerza espacial deben continuar evolucionando en un modelo de comunicación interdependiente. Ese paso intermedio es necesario para hacer la transición de guerra cibernética de una misión principalmente de USCYBERCOM a una misión compartida entre USCYBERCOM y los GCCs. El siguiente elemento constitutivo, un modelo interdependiente, le permitiría a cada GCC elaborar una capacidad orgánica naciente de guerra cibernética y crear expertos regionales en guerra cibernética.

Las operaciones interdependientes se diferencian de las operaciones independientes en que ambas partes dependen de cada una para el logro de la misión. Las operaciones interdependientes son más complejas que las operaciones independientes porque requieren coordinación para evitar la duplicación de esfuerzo y maximizar la utilidad. Las acciones de guerra cibernética que ocurren a casi una "velocidad de red" exigirán planificación y coordinación detalladas porque la velocidad de ejecución podría tornar imposible la comunicación en tiempo real. Las operaciones de movilidad aérea ofrecen conocimientos sobre cómo mitigar los retos de comunicación de las operaciones interdependientes.

En vista de los recursos limitados de movilidad aérea, las operaciones globales de movilidad aérea deben ocurrir interdependientemente entre el FCC, USTRANSCOM y los GCCs. El DOD sencillamente no cuenta con suficientes recursos de movilidad aérea para darle a cada GCC todo el transporte aéreo que requieren. Por lo tanto, todos los componentes deben compartir la propiedad y colaborar. Por este motivo, la "propiedad" de la fuerza de movilidad aérea puede ser dividida en tres clasificaciones específicas: aquellas fuerzas bajo el mando de USTRANSCOM, aquellas para el GCC (tales como el Comando de EE.UU. en el Pacífico) y las fuerzas de movilidad aérea orgánicas de cada servicio armado.[18]

USTRANSCOM mantiene un componente aéreo, Transporte de las Fuerzas Aéreas de EE.UU., que, a su vez, mantiene el 618º AOC. Este último, que se comunica a diario con los AOCs del GCC para permitir las operaciones globales de movilidad, tiene la responsabilidad

de la mayoría del transporte aéreo entre los teatros de operaciones, mientras que los AOCs de los GCCs son responsables por la mayoría del transporte aéreo dentro del teatro de cada GCC.[19] Por lo tanto, el 618º AOC y los AOCs del GCC trabajan interdependientemente para garantizar el éxito de la iniciativa de la movilidad aérea global.

La doctrina conjunta ofrece el concepto de un facilitador para ayudar este proceso. En el JP 3-17, *Air Mobility Operations* (Operaciones de Movilidad Aérea), se define al director de las fuerzas de movilidad (DIRMOBFOR) como una "autoridad coordinadora para la movilidad aérea con todos los comandos y agencias, tanto internas como externas a la JTF (fuerza de tarea conjunta), inclusive el JAOC (centro conjunto de operaciones aéreas), el 618º TACC (Centro Táctico de Control Aéreo, conocido ahora como el 618º AOC), y el JDDOC (centro conjunto de despliegue y operaciones de distribución) o el JMC (centro conjunto de movilización)"[20]. En el JP 3-17 se describe al DIRMOBFOR como "por lo regular un oficial superior que está familiarizado con la zona de responsabilidad (AOR, por sus siglas en inglés) o la zona de operaciones conjuntas (JOA, por sus siglas en inglés) y posee una amplia experiencia en operaciones de movilidad aérea. El DIRMOBFOR se desempeña en calidad de agente para todos los asuntos de movilidad aérea en la AOR o JOA, y para otras tareas según se le ordene".[21] Sin embargo, en vista de que el DIRMOBFOR representa al comandante de las fuerzas de la Fuerza Aérea en lugar de al comandante del componente aéreo de la fuerza conjunta, el director debe trabajar con el comandante del AOC y su división de movilidad aérea para las operaciones de transporte dentro del teatro. Dentro del AOC del teatro, la división de movilidad aérea "integrará y dirigirá la ejecución de las fuerzas de movilidad orgánicas del servicio asignadas o adscritas al teatro en la AOR o JOA en apoyo a los objetivos del comandante de la fuerza conjunta (JFC, por sus siglas en inglés)".[22] El 618º AOC trabaja interdependientemente con el DIRMOBFOR del GCC y el AOC para garantizar que el guerrero recibe apoyo vía las actividades de transporte y por ende obtiene la logística necesaria (alimentos, municiones y personal).

Logrando la acción interdependiente del USCYBERCOM: Director de las Fuerzas Cibernéticas. La CCA del GCC debe convertirse en el equivalente del DIRMOBFOR para las capacidades de guerra cibernética (por ejemplo, un DIRCYBERFOR). El DIRCYBERFOR continuaría trabajando con el USCYBERCOM, como lo hizo el CCA, para las capacidades externas de guerra cibernética pero también trabajaría con los guerreros cibernéticos orgánicos nacientes del GCC a través de los canales C2 orgánicos en el teatro. En este segundo paso, los GCCs desarrollarían la capacidad de guerra cibernética inicial que requeriría C2 dentro del GCC en sí—ajena al USCYBERCOM. A diferencia de la CCA, el DIRCYBERFOR cuenta con una plantilla doctrinal en la ubicación del DIRMOBFOR bajo el comandante de las fuerzas de la Fuerza Aérea. Aunque los procesos requeridos para integrar el transporte aéreo difieren claramente de los procesos para integrar las actividades de tiro no cinético del USCYBERCOM, el concepto de un DIRCYBERFOR tiene valor.

La doctrina conjunta ofrece la siguiente pauta a los JFCs que organizan componentes funcionales: "Por lo regular, el CDR del componente del servicio con la preponderancia de las fuerzas a las que se les asignan las tareas y la capacidad de C2 de esas fuerzas, será designado como el CDR del componente funcional. Sin embargo, el JFC siempre tomará en cuenta la misión, naturaleza y duración de la operación, las capacidades de la fuerza y las capacidades de C2 al seleccionar un CDR".[23] Las fuerzas CNA/CND-RA están en tal estado de formación que los GCCs tendrán dificultad en determinar a quién designar como el DIRCYBERFOR. Aunque no están basadas en tierra directamente, puede que sea mejor para el CCA y el DIRCYBERFOR comenzar al nivel de JFC y luego hacer la transición con el transcurso del tiempo para crear un componente cibernéticamente funcional tanto al nivel GCC como al JFC en el futuro.

Logrando la acción interdependiente del USCYBERCOM: Elemento de Guerra Ciber-

nética. El proceso de la división de movilidad aérea del AOC podría servir de modelo para una estructura C2 en el teatro para las fuerzas cibernéticas incipientes—un elemento de guerra cibernética (CWE, por sus siglas en inglés). Mientras que una división de movilidad aérea se esfuerza por dirigir y ejecutar la misión de transporte aéreo orgánica del JFAC, el CWE se esforzaría por dirigir y ejecutar la misión de guerra cibernética del JFC. A medida que los JFCs buscan integrar las capacidades de guerra cibernética dentro del esquema de la maniobra del teatro, un CWE pequeño podría reportarse al DIRCYBERFOR dentro del personal del JFC.

En este momento, debemos hacer una advertencia. El primer paso, el modelo espacial, implicaba enviar defensores para ayudar al guerrero a presentar sus requerimientos al USCYBERCOM a través de la SCA. El segundo paso, el modelo de movilidad aérea, no puede remover subsiguientemente esas fuerzas y usarlas como la base para organizar CWEs porque cada componente del GCC aún necesitará defensores de la guerra cibernética para promocionar los requerimientos del guerrero al CWE y al DIRCYBERFOR.

Logrando la acción interdependiente del USCYBERCOM: Centro de Operaciones Cibernéticas. A medida que las fuerzas se tornan más asequibles para establecer los CWEs, el USCYBERCOM debe establecer un centro de operaciones cibernéticas utilizando el 618º AOC como modelo para interactuar con los GCCs. El centro trabajará con los CWEs del GCC y los DIRCYBERFORs para darle prioridad, distribuir, asignar y utilizar las capacidades globales de la guerra cibernética.

Tercer Paso: Un modelo USSOCOM—Acción Orgánica

Durante un testimonio ante el Congreso, el General Alexander destacó que

> El mando y control en el ciberespacio es aún más complicado (que en otros ámbitos). Las operaciones en la red de computadoras pueden ser regionales y globales al mismo tiempo, y pueden tener resultados que se aproximan a los de las armas de destrucción en masa. Los dispositivos que nos permiten el acceso al ciberespacio existen en el mundo físico, y en términos militares convencionales podemos decir que siempre están dentro del área de responsabilidad de algún comando combatiente geográfico—pero pueden crear efectos que ocurren lejos del área de responsabilidad de un segundo comando, y puede que usuarios confiados y sus dispositivos ubicados aún en la región de un tercer comando les permitan hacerlo. En ese caso ¿cuál es el comandante a cargo de la misión y es la acción militar la correcta? ¿Cuál comando recibe apoyo y cuál da el apoyo? En el ciberespacio, preguntas como estas se deben responder a la velocidad de la Internet y deben tomar en cuenta nuestras responsabilidades y obligaciones bajo la ley y las normas internacionales.[24]

Los retos que el General Alexander describió son desalentadores, pero no son únicos—de hecho, son bastante similares a los retos que enfrentamos cuando combatimos el terrorismo y llevamos a cabo operaciones especiales en general. El DOD ha analizado minuciosamente el terrorismo y ha determinado que el mejor método para confrontar este reto global es ordenarle al USSOCOM a que "sincronice la planificación de las operaciones globales contra las redes terroristas".[25] En vista de los retos similares enfrentados al librar la guerra cibernética y por las SOF, el USCYBERCOM a la larga debería adoptar los modelos de presentación de fuerzas y de C2 del USSOCOM.

USSOCOM ha optado por colar fuerzas tanto globalmente desde el territorio continental de Estados Unidos y regionalmente (orgánicamente) dentro de los GCCs. A diferencia de las fuerzas de apoyo, las fuerzas orgánicas son el concepto doctrinal para la presentación de fuerzas del GCC en tiempo de guerra, según se define en el JP 1, *Doctrine for the Armed Forces of the United States* (Doctrina de las Fuerzas Armadas de Estados Unidos).[26] Con base en ese documento, algún tipo de fuerzas cibernéticas orgánicas también deben ser la meta final para la presentación de fuerzas y de C2 del GCC.

Al igual que las operaciones especiales, librar guerras en el ciberespacio es tanto global como regional por naturaleza. La comunidad de SOF ha tratado la doble naturaleza global y regional del terrorismo y ha elaborado una ar-

quitectura C2 y un modelo para la presentación de fuerzas que le proveen al USCYBERCOM perspicacias singulares y relevantes. Todas las fuerzas SOF acantonadas en el territorio continental de Estados Unidos caen bajo la autoridad de mando del USSOCOM, mientras que aquellas asignadas a un GCC caen bajo la autoridad del comandante del GCC. En su condición de FCC, el USSOCOM provee fuerzas adicionales de manera temporal a los GCCs para el empleo operacional, con el GCC por lo regular ejerciendo control operacional sobre ellas.[27] El GCC ejerce C2 sobre todas las fuerzas especiales asignadas y adscritas a través de un comando de operaciones especiales en el teatro (TSOC, por sus siglas en inglés), que provee unidad de mando y sirve como "la organización SOF principal capaz de llevar a cabo misiones continuas y amplias singularmente aptas para las capacidades SOF" y "el mecanismo principal mediante el cual un comandante combatiente geográfico ejerce C2 sobre el SOF".[28] El comandante del TSOC desempeña tres funciones principales: JFC del SOF en el teatro, asesor de operaciones especiales en el teatro, y comandante del componente conjunto de las fuerzas de operaciones especiales.[29] Esta "triple función" hace que el puesto sea singular dentro de los GCCs. Solamente este comandante tiene doble responsabilidad como un JFC; los componentes del servicio del GCC tienen doble responsabilidad en calidad de comandantes del componente porque los componentes del servicio, a diferencia del SOF, intrínsecamente no son conjuntos.

Logrando la acción orgánica del USCYBERCOM: Comando de Operaciones Cibernéticas en el Teatro. El USCYBERCOM debe adoptar una mentalidad de proveedor de fuerza USSOCOM para cada componente bélico cibernético orgánico del GCC. Cada teatro de operaciones establecería un comando de operaciones cibernéticas en el comando (TCYOC, por sus siglas en inglés) para proveer el mismo tipo de apoyo y C2 provisto por el TSOC para la SOF. El comandante del TCYOC se desempeñaría como el JFC para todo el personal asignado y adscrito de operaciones cibernéticas, en calidad de asesor de operaciones cibernéticas en el teatro y en calidad de comandante del componente conjunto de operaciones cibernéticas. Poner en vigor este concepto evidentemente elevaría el ciberespacio a un nivel de importancia apropiado.

Logrando la acción orgánica del USCYBERCOM: Componente Conjunto de Ataque Cibernético. Las capacidades orgánicas CNA de múltiples servicios se deben combinar bajo un componente conjunto de ataque cibernético. La doctrina conjunta provee pautas sobre cómo el TCYOC debe presentar las fuerzas al GCC: "Los comandos del componente funcional son apropiados cuando fuerzas de dos o más departamentos militares deben operar dentro de la misma zona de la misión o ámbito geográfico o cuando hay una necesidad de lograr un aspecto específico de la misión asignada".[30] Si múltiples servicios proveen capacidades de ataque cibernético y respuesta defensiva dentro del TCYOC, sería apropiado crear componentes funcionales para cada uno. Por ejemplo, en el JP 3-05, *Doctrine for Joint Special Operations* (Doctrina para las Operaciones Especiales Conjuntas), se discute cómo un componente aéreo conjunto de operaciones especiales a menudo se establece dentro de una fuerza de tarea conjunta de operaciones especiales cuando múltiples servicios cuentan con recursos aéreos orgánicos.[31] Este componente crea una capa de supervisión sobre varios elementos SOF de aviación de manera que el recurso limitado se pueda emplear de la manera más eficaz.

En el futuro, un TCYOC probablemente contará con componentes orgánicos de los servicios. La plantilla SOF ilustra un escenario en el cual múltiples servicios podrían ofrecer capacidades que coinciden. Aunque muchos aspectos SOF están conectados singularmente a un componente del servicio, capacidades tales como la movilidad aérea y ataques aerotransportados radican en dos componentes del servicio armado. Las lecciones aprendidas de las operaciones en el teatro dieron lugar al concepto doctrinal de un componente aéreo conjunto de operaciones especiales en el teatro de operaciones.

Si las capacidades CNA/CND-RA del servicio evolucionaron en funciones especializadas, un estudio de la doctrina SOF indicaría

que los componentes cibernéticos del servicio deben ser adecuados. No obstante, traslapar algunos de los aspectos de las capacidades CNA/CND-RA provistas por los servicios puede que amerite una capa adicional de C2.

Logrando la acción orgánica del USCYBERCOM: Elementos de Enlace. El componente bélico cibernético del GCC debe enviar elementos de enlace a otros componentes funcionales. Cada GCC mantiene un componente de operaciones especiales que debe enlazarse con los otros componentes del GCC (o fuerza de tarea conjunta subordinada). Según el JP 3-05, "Para poder integrar completamente las operaciones especiales (SO, por sus siglas en inglés) y las operaciones convencionales, la SOF debe mantener un enlace eficaz con todos los componentes de la fuerza conjunta para garantizar que la unidad de esfuerzo se mantiene y se minimiza el riesgo de fratricidio".[32] En la doctrina de operaciones especiales se tratan aspectos en los que el SOF debe enviar elementos de enlace:

> Los comandantes SOF tienen disponibles elementos específicos que facilitan C2, coordinación y enlace. Estos incluyen…el elemento de enlace de operaciones especiales…para proveer enlace al comandante del componente aéreo de la fuerza conjunta…o la instalación aérea C2 apropiada del componente del servicio y oficiales de enlace SOF (LNOs, por sus siglas en inglés) colocados en una variedad de lugares según sea necesario para coordinar, sincronizar y armonizar las SO dentro del área operacional… Todos estos elementos mejoran significativamente el flujo de información, facilitan la planificación simultánea y mejoran el logro de la misión en general de la fuerza conjunta.[33]

El TSOC integra el personal dentro del AOC para coordinar, armonizar e integrar las operaciones aéreas, de superficie y debajo de la superficie de la SOF.[34] La doctrina de las operaciones especiales reconoce que la comunicación entre los componentes orgánicos dentro del GCC exigen un esfuerzo deliberado y la distribución de recursos.

Logrando la acción orgánica del USCYBERCOM: Elementos de Enlace de Guerra Cibernética. El USCYBERCOM debería estudiar crear elementos de enlace de guerra cibernética al buscar los TCYOCs. En el JP 3-05 se discute cómo el elemento de enlace de las operaciones especiales se integra dentro del JAOC.[35] Los integrantes de éste ultimo se integran en los procesos en todo el AOC. De manera similar, los elementos de enlace de la guerra cibernética podrían integrar capacidades de guerra cibernética dentro de las diferentes divisiones del JAOC. Por ejemplo, en caso de que el TCYOC planificara una acción CNA/CND-RA significativa, los elementos de enlace podrían garantizar la integración y la armonización correcta de la actividad dentro de los procesos JAOC.

Logrando la acción orgánica del USCYBERCOM: Responsabilidades "Parecidas a las del Servicio". Al USCYBERCOM se le deben otorgar las responsabilidades apropiadas "parecidas a las del servicio" para requerimientos cibernéticos específicos modelados a imagen del USSOCOM. En la metodología para la presentación de fuerzas SOF se trata la presentación de fuerzas tanto desde la perspectiva del COCOM como del servicio. USSOCOM tiene responsabilidades parecidas a las del servicio en que organiza, capacita y equipa a la SOF. [36] Esto incluye mantener su propio programa de fuerza principal para obtener equipo especializado. Por ejemplo, la USAF compra un Hércules C-130 y se lo entrega al Comando de Operaciones Especiales de la USAF, el que a su vez "moderniza" al C-130 en un avión armado AC-130U Spooky. Un beneficio de este arreglo es que los requerimientos específicos de la SOF (indistintamente del servicio involucrado) recibirá una cantidad de apoyo apropiada y no será opacado por los requerimientos en disputa a nivel de servicio. Análogamente, el USCYBERCOM debe ser el principal FCC del DOD para organizar, capacitar y equipar a las fuerzas CNA y CND-RA.

Aparte del USSOCOM, equipar y capacitar a sus miembros es función de los servicios. Los servicios armados tienden a desarrollar y adquirir capacidades según sus propias prioridades, las que no necesariamente favorecen decisiones optimizadas para las operaciones ciberespaciales. Además, el ciberespacio es intrísecamente una zona de operaciones conjuntas (o inclusive interagencial), sin embargo

los servicios podrían buscar soluciones técnicas diferentes para realizar capacidades similares, tales como *software* CNA. Puede que también surjan brechas en la investigación, desarrollo y adquisición. Con responsabilidades similares a las del servicio, el USCYBERCOM podría ofrecer apoyo específico al ciberespacio para los sistemas de adquisición, investigación y desarrollo.

Logrando la acción orgánica del USCYBERCOM: Universidad Conjunta de Operaciones Ciberespaciales. Para capacitar, o en este caso, educar a sus miembros, el USCYBERCOM debería crear una Universidad Conjunta de Operaciones Ciberespaciales parecida a la Universidad Conjunta de Operaciones Especiales. USSOCOM mantiene esta última para ofrecer educación continua a la SOF a nivel mundial. La Universidad se enfoca en formar a líderes superiores e intermedios y formuladores de política selectos que no pertenecen a las operaciones especiales (tanto militares como civiles) en las operaciones especiales conjuntas.[37] La Universidad Conjunta de Operaciones Ciberespaciales podría desempeñar un papel importante en la formación de futuros líderes ciberespaciales. Podría asociarse con las escuelas de los servicios de la misma manera que la Universidad Conjunta de Operaciones Especiales se asocia con esas escuelas, inclusive la Escuela de Operaciones Especiales de la USAF. [38] Además, el USCYBERCOM podría sacarle provecho a unos cuantos programas de educación y adiestramiento cibernético, inclusive la Escuela de la Fuerza Aérea de Adiestramiento Cibernético, el Instituto de Tecnología de la Fuerza Aérea y la Escuela de Posgrado de la Armada.[39] Puede que hasta sea posible implementar la Universidad Conjunta de Operaciones Ciberespaciales de una manera descentralizada. Escuelas nuevas que tratan específicamente con la conducción de la guerra en el ciberespacio, tales como una Escuela Ciberespacial de Estudios Avanzados Aéreos y Espaciales y un Curso para Instructores de Armamento Cibernético dentro de la Escuela de Armamento de la USAF también podrían cumplir con los requerimientos específicos del USCYBERCOM.[40]

Conclusión

Hoy el USCYBERCOM podría comenzar la implementación de un método progresivo para normalizar la presentación de la fuerza para la conducción de la guerra cibernética y C2. Cada paso tomaría como punto de partida las medidas tomadas en el paso anterior. El primer paso, tomar las lecciones aprendidas del espacio, requeriría poco personal adicional. Inicialmente, el USCYBERCOM abogaría porque los GCCs adoptaran la autoridad coodinadora cibernética para la presentación de la fuerza cibernética. Simultáneamente, el USCYBERCOM le ordenaría a sus componentes del servicio que enviaran defensores de guerra cibernética a los respectivos componentes GCC del servicio y funcionales con el fin de integrar mejor la contribución del USCYBERCOM a las actividades de conducción de la guerra del GCC.

El segundo paso en el método progresivo implicaría la transición de un modelo espacial a un modelo de movilidad aérea. El CCA del paso anterior evolucionaría en un DIRCYBERFOR para las actividades bélicas cibernéticas. A medida que haya fuerzas disponibles, los GCCs establecerían elementos para la conducción de la guerra cibernética y el USCYBERCOM establecería un centro de operaciones cibernéticas para que interactúe con los GCCs.

Dentro del modelo de movilidad aérea, los defensores de la conducción de la guerra cibernética del USCYBERCOM permanecerían subordinados a los demás componentes del GCC, al igual que estaban bajo el modelo espacial. No obstante, dentro del modelo USSOCOM, estos defensores del USCYBERCOM se convertirían en enlaces del componente de guerra cibernética del GCC a otros componentes del GCC. Con este método progresivo, los individuos permanecerían, pero su cadena C2 cambiaría del USCYBERCOM al GCC.

En el tercer paso (el modelo USSOCOM), la relación entre el personal JFC del teatro y el centro C2 del USCYBERCOM evolucionarían a uno de un FCC responsable por las operaciones globales de la conducción de la guerra cibernética y un componente bélico ciberné-

tico del GCC a cargo de las actividades regionales de la conducción de la guerra cibernética. El centro C2 del USCYBERCOM también mantendría la responsabilidad de sincronizar las acciones regionales entre los GCCs. Esta responsabilidad de sincronización exigiría una coordinación estrecha entre los componentes cibernéticos del GCC y el centro C2 del USCYBERCOM.

USSOCOM ha utilizado sus responsabilidades "similarea a las de los servicios" para promover las capacidades bélicas de las operaciones especiales. Adaptar los atributos "similares a los de los servicios" del USSOCOM podría ayudar al USCYBERCOM prácticamente de la misma manera. La importancia de la educación en crear una fuerza bélica cibernética no se puede exagerar, y la Universidad Conjunta de Operaciones Especiales ofrece un modelo que el USCYBERCOM puede adaptar.

Si bien el DOD aún lucha con el sólo concepto de la conducción de la guerra en el ciberespacio y aún no está claro sobre cuáles acciones constituirían actos de guerra, aún tiene que tratar el tema de cómo presentar fuerzas cibernéticas y ejercer el C2 de ellas. El ciberespacio es definitivamente un ámbito por el cual luchar, pero ¿acaso es uno singular? Aunque algunos aspectos del ciberespacio son indudablemente singulares, argumentamos que en el campo de presentación de la fuerza y de C2, el ciberespacio es análogo a otros ámbitos bélicos; por ende, podemos aplicar lecciones del espacio y de las operaciones aéreas al ciberespacio. Por lo tanto, recomendamos que el USCYBERCOM adopte nuestro anteproyecto basado en la doctrina para presentar y ejercer C2 de las fuerzas bélicas cibernéticas. ❑

Base Aérea Scott, Illinois
Base Aérea Wright-Patterson, Ohio

Notas

1. La doctrina conjunta define el *ciberespacio* como un ámbito global. Consultar la Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Publicación Conjunta [JP, por sus siglas en inglés] 1-02, Diccionario de Términos Militares y Afines del Departamento de Defensa), 12 de abril de 2001 (según enmendado hasta el 30 de septiembre de 2010), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. Air Force Doctrine Document 3-12, *Cyberspace Operations* (Documento de Doctrina de la Fuerza Aérea [AFDD, por sus siglas en inglés], Operaciones Ciberespaciales), 15 de julio de 2010, 14, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf.

3. JP 3-13, *Information Operations* (Operaciones de Información), 13 de febrero de 2006, IV-5, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

4. Lt Gen Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly* 46 (Third Quarter 2007) (La conducción de la guerra en el ciberespacio): 60, https://digitalndulibrary.ndu.edu/cgi-bin/showfile.exe?CISOROOT=/ndupress&CISOPTR=20001&CISOMODE=print.

5. En el JP 1-02, *Department of Defense Dictionary* (Diccionario del Departamento de Defensa), se define *ataque a la red de computadoras* como "medidas tomadas a través del uso de las redes de computadoras para interrumpir, degradar o destruir información que radica en las computadoras y redes de computadoras, o en las computadoras y las redes en sí" (93); *defensa de la red de computadoras* como "medidas tomadas para proteger, vigilar, analizar, detectar y responder a una actividad no autorizada dentro de los sistemas de informática y las redes de computadora del Departamento de Defensa" (93); y *aprovechamiento de la red de computadoras* como "operaciones facilitadoras y capacidades de recopilación de inteligencia llevadas a cabo a través del uso de las redes de computadoras para recopilar datos de sistemas de informática automatizados o redes consideradas blancos o del adversario" (93).

6. CND-RAs son "medidas o actividades de defensa deliberadas y autorizadas que protegen y defienden los sistemas y las redes de computadoras del DOD que están bajo ataque o han sido seleccionadas para ser atacadas por los sistemas/redes de computadoras del adversario. Las RAs amplían las capacidades de defensa profundas y aumentan la aptitud del DOD de soportar los ataques del adversario". Chairman of the Joint Chiefs of Staff Instruction 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND)* (Instrucción del Presidente de la Junta del Estado Mayor Conjunto 6510.01E, Seguridad de la Información [IA, por sus siglas en inglés] y Defensa de las Redes de Computadoras [CND, por sus siglas en inglés]), 12 de agosto de 2008, GL-7, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf.

7. JP 3-13, *Information Operations* (Operaciones de Información), IV-5.

8. JP 6-0, *Joint Communications System* (Sistema Conjunto de Comunicaciones), 10 de junio de 2010, III-1, http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

9. Para una discusión más profunda sobre la importancia de separar la conducción de la guerra en el ámbito de las medidas tomadas para conservar acceso al ámbito, consultar al Dr. Robert F. Mills, Mayor M. Bodine Birdwell y Mayor Kevin R. Beeker, "Apples & Oranges: Operating and Defending the Global Information Grid (Peras y Manzanas: Operando y Defendiendo la Red Global de Información)," *IAnewsletter* 13, no. 2 (Primavera 2010): 39–40, http://iac.dtic.mil/iatac/download/Vol13_No2.pdf.

10. Alexander, "Warfighting in Cyberspace," 60.

11. JP 1, *Doctrine for the Armed Forces of the United States* (Doctrina para las Fuerzas Armadas de Estados Unidos), 2 de mayo de 2007 (incorporando el cambio 1, 23 de marzo de 2009), ii, III-12–13, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

12. General Kevin Chilton, "Remarks to the November 2008 Air Force Association Global Warfare Symposium" (Comentarios ante el Simposio de la Asociación de la Fuerza Aérea sobre la Guerra Global, noviembre de 2008) http://www.stratcom.mil/speeches/17/.

13. JP 3-14, *Space Operations* (Operaciones Espaciales), 6 de enero de 2009, III-2, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

14. Ibid.

15. Ibid., IV-7–8.

16. Ibid., IV-8–11.

17. JP 3-05, *Doctrine for Joint Special Operations* (Doctrina para las Operaciones Especiales Conjuntas), 17 de diciembre de 2003, IV-7, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf.

18. JP 3-17, *Air Mobility Operations* (Operaciones de Movilidad Aérea), 2 de octubre de 2009, I-7, 9, http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf.

19. Ibid., II-2.

20. Ibid., II-4.

21. Ibid., II-4–5.

22. Ibid., II-8.

23. JP 1, *Doctrine for the Armed Forces of the United States*, V-19.

24. House, *Statement of General Keith B. Alexander, Commander, United States Cyber Command, before the House Committee on Armed Services, 23 September 2010* (Declaración del General Keith B. Alexander, Comandante del Comando Cibernético de EE.UU., ante el Comité de Servicios Armados de la Cámara de Representantes), 111th Cong., 2nd sess., 6–7, http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf.

25. "Mission of U.S. Special Operations Command" (Misión del Comando de Operaciones Especiales de Estados Unidos), consultado el 24 de septiembre de 2010, http://www.socom.mil/SOCOMHome/Pages/About.aspx.

26. JP 1, *Doctrine for the Armed Forces of the United States*, III-12, 13.

27. JP 3-05, *Doctrine for Joint Special Operations*, III-2, 3.

28. Ibid., III-4.

29. Ibid.

30. JP 1, *Doctrine for the Armed Forces of the United States*, V-4.

31. JP 3-05, *Doctrine for Joint Special Operations*, III-9.

32. Ibid., viii.

33. Ibid., III-10.

34. Ibid., III-12.

35. Ibid.

36. Ibid., III-2.

37. Ibid., A-1.

38. Para más información básica sobre la escuela, consultar "U.S. Air Force Special Operations School, (Escuela de Operaciones Especiales de la Fuerza Aérea)" Air Force Special Operations Command (Comando de Operaciones Especiales de la Fuerza Aérea), consultado el 10 de noviembre de 2010, http://www.afsoc.af.mil/usafsos/.

39. Consultar "New Undergraduate Cyber Training School Opens (Nueva Escuela de Adiestramiento Cibernético abre sus Puertas)," 17 de junio de 2010, consultado el 6 de diciembre de 2010, http://www.keesler.af.mil/news/story.asp?id=123209936; "Graduate School of Engineering and Management, Center for Cyberspace Research (CCR)" (Escuela de Posgrado de Ingeniería y Administración, Centro de Investigaciones Ciberespaciales [CCR, por sus siglas en inglés]), consultado el 10 de noviembre de 2010, http://www.afit.edu/en/ccr/; y "Center for Cyber Warfare Established at NPS" (Se establece en NPS Centro para la Guerra Cibernética), consultado el 10 de noviembre de 2010, http://www.nps.edu/Academics/Institutes/Cebrowski/News-and-Events/cybersummit/docs/CyberCenter.pdf.

40. Mayor Paul D. Williams, "Cyber ACTS/SAASS: A Second Year of Command and Staff College for the Future Leaders of Our Cyber Forces" (ACTS/SAASS Cibernético: Un segundo año de Escuela Superior de Comando y Estado Mayor para los futuros líderes de nuestras fuerzas cibernéticas), *Air and Space Power Journal* 23, no. 4 (Invierno de 2009): 21–29, http://www.airpower.au.af.mil/airchronicles/apj/apj09/win09/win09.pdf.

El Teniente Coronel (USAF) M. Bodine Birdwell es director de operaciones, Escuadrón de Inteligencia Aérea, Comando de Movilidad Aérea, Base Aérea Scott, Illinois. Es graduado distinguido del programa de Guerra Cibernética del Instituto de Tecnología de la Fuerza Aérea y egresado de la Escuela de Armamento de la Fuerza Aérea.

El Teniente Coronel (USAF-Ret.) Robert Mills, PhD es Profesor Adjunto de Ingeniería Eléctrica en el Instituto de Tecnología de la Fuerza Aérea y catedrático de currículo para el programa de Formación Educacional Intermedia de Guerra Cibernética de AFIT. Se retiró del servicio activo en el 2003 después de haber servido 21 años en calidad de oficial de comunicaciones/radares.