

La Importancia de Designar Sistemas de Armas Ciberespaciales

GENERAL DE BRIGADA ROBERT J. SKINNER, USAF

La publicación conjunta 1-02-, Department of Defense Dictionary of Military and Associated Terms (Diccionario de Términos Militares y Relacionados del Departamento de Defensa), define un sistema de armas como “una combinación de una o más armas con todos los equipos, materiales, servicios, personal y medios de suministro y despliegue relacionados (si corresponde) requeridos para la autosuficiencia”.¹ Cuando uno piensa en la Fuerza Aérea de EE.UU. y de los sistemas de armas, el bombardero furtivo B-2 Spirit, el avión F-15E Strike Eagle o el avión F-16 Fighting Falcon se vienen rápidamente a la cabeza. Incluso el misil Minuteman III, el Sistema de Posicionamiento Global o el avión de reabastecimiento de combustible de aire KC-135 Stratotanker podría convertirse en parte del debate, después de todo, la misión de la Fuerza Aérea es volar, luchar y ganar en el aire, espacio y ciberespacio. Estos haberes, que están comprendidos bajo el paraguas del aire y del espacio, han servido como sistemas de armas de eficacia demostrada durante muchos años. La Fuerza Aérea se ha añadido ahora a la larga línea de sus sistemas de armas que apoyan operaciones ciberespaciales “el empleo de capacidades ciberespaciales donde la finalidad principal es lograr objetivos en, de, o a través del ciberespacio”. Estos sistemas son únicos por el hecho de que están unidos al dominio cibernético más reciente—“un dominio global dentro del entorno de información consistente en una red interdependiente de infraestructuras de tecnología de información y datos residentes, incluida Internet, las redes de telecomunicaciones, los sistemas de computadoras y los procesadores y controladores empotrados”.

El 24 de marzo de 2013, el jefe de estado mayor de la Fuerza Aérea aprobó la designación oficial de seis sistemas de armas ciberespaciales bajo el liderazgo del Mando Espacial de la Fuerza Aérea (AFSPC), que es responsable de organizar estos sistemas, equipar las unidades con ellos y adiestrar a los individuos para que usen los sistemas. La estipulación de la Fuerza Aérea de alcance, poder y vigilancia globales entre los dominios del aire y del espacio se aplica ahora a los dominios ciberespaciales mediante la designación de los siguientes sistemas de armas ciberespaciales:

- Defensa del Ciberespacio de la Fuerza Aérea.
- Análisis de Defensa del Ciberespacio .
- Evaluación de Vulnerabilidad/Búsqueda en el Ciberespacio.
- Control de la Red Interna de la Fuerza Aérea.
- Sistema de Seguridad y Control Cibernéticos de la Fuerza Aérea.
- Sistema de Misiones de Mando y Control Cibernéticos.

Aunque los nombres pueden implicar cierta duplicación del esfuerzo con respecto a estas capacidades, el personal y los equipos que comprenden estos sistemas efectúan misiones exclusivas y se complementan entre sí. Todos ellos se concentran en proporcionar y asegurar el ciberespacio como un habilitador de misiones y proteger información crítica mientras se defienden nuestras redes contra los ataques. Cualquier consideración de las capacidades de estos sistemas de armas se beneficiarían de comparar este conjunto de sistemas de armas ciberespaciales con los sistemas de armas de transporte aéreo militar de la Fuerza Aérea (C-5, C-17, C-130, etc.), cada uno de los cuales contribuye de forma exclusiva a la misión de movilidad aérea general. Así como existen distinciones claras entre estas plataformas, basándose en las capacidades operacionales requeridas, también difieren los sistemas de armas ciberespaciales entre sí. Los sistemas pueden tener áreas de misiones superpuestas, pero son complementarios de forma muy parecida a como lo son nuestras plataformas de transporte aéreo—ofrecen capacidades completas.

Las revelaciones de actividades chinas en nuestras redes, según se describió anteriormente este año en el informe de Mandiant Company titulado *Advanced Persistent Threat (APT) 1: Exposing One of China's Cyber Espionage Units (Amenaza Persistente Avanzada (APT) 1: Exposición de una de las unidades de espionaje cibernético de China)*, subraya la necesidad urgente de que la Fuerza Aérea y la nación desarrollen capacidades para defender este dominio crítico y asegurar así la superioridad de la información. El informe ilustra la amenaza persistente, observando que “los detalles que hemos analizado durante cientos de investigaciones nos convencen de que los grupos que llevan a cabo estas actividades se basan principalmente en China y que el gobierno chino es consciente de ellas. . . . Nuestro análisis nos ha llevado a la conclusión de que APT1 probablemente está patrocinado por el gobierno y uno de los actores de amenazas cibernéticas más persistentes de China”. El informe Mandiant en APT 1 resalta solamente uno de más de 20 grupos de APT basados en China, haciendo el seguimiento de este grupo individual a ciberataques contra casi 150 víctimas en más de siete años con cientos de terabytes de datos exfiltrados.² Claramente, esta conversación no se confina a ningún adversario en particular. Muchos agresores habitan el dominio ciberespacial, y el ejecutor de estas actividades varía desde un individuo en el sótano de su casa hasta grupos de individuos que cooperan en equipos, para naciones estado. Sus intenciones también pueden abarcar un espectro de actividades, incluidas espionaje, robo de capital intelectual, crimen organizado, robo de identidades, operaciones militares, y así sucesivamente.

Este artículo examina cada sistema de armas, resalta su historia y capacidades exclusivas, y describe las unidades específicas que operan el sistema. Después, trata de la importancia de clasificar estas capacidades como “sistemas de armas”, indicando como tratan directamente a las amenazas a las que nos enfrentamos hoy. No obstante, antes de hacer eso, el artículo presenta una viñeta de creación de un escenario para establecer un entendimiento de capacidades de sistemas de armas y su empleo contra un adversario.

Suponga que usted es un funcionario civil del gobierno sentado en su despacho en una sede de mando importante cuando recibe un correo electrónico relacionado con el secuestro y un despido temporal potencial de su trabajo. En este correo electrónico se incluye un enlace a un sitio web para obtener información adicional. Trata de abrir el enlace pero recibe un mensaje de error. Lo intenta nuevamente y obtiene el mismo resultado. Después reanuda el trabajo en sus tareas. Sin saberlo, el enlace le ha dirigido a un servidor de un sitio web malicioso que descargó malware que permitía a un adversario asumir el control de su computadora de despacho. ¿Cómo podría ocurrir esto, y por qué hay alguien que se fija específicamente en usted? Realmente no fue difícil. ¿Recuerda el congreso al que asistió hace unos cuantos meses, antes de que se limitara la ubicación temporal de funciones? El adversario copió su dirección de correo electrónico de la hoja de inscripción del congreso, que también estaba a disposición de los patrocinadores del suceso. ¿Por qué usted? Los adversarios consideran que sus conocimientos expertos exclusivos y acceso a información valiosa es un “entorno rico en objetivos”. Solamente una persona necesita hacer clic en el enlace para iniciar una serie de acciones maliciosas. Como el adversario no dejó ninguna pista de un problema en su computadora, ahora tiene acceso sin trabas a esa información no secreta pero útil.

¿Cómo combate la Fuerza Aérea dichas intrusiones? Realmente, la mejor defensa para los ataques de suplantación de identidad es educar a los usuarios. No obstante, estos ataques se están haciendo más refinados y a veces es casi imposible identificarlos. Todos los servicios tienen unidades ciberespaciales responsables de la defensa de la red. En este caso, el monitoreo de tráfico de la red alerta a la Fuerza Aérea sobre la intrusión en la computadora de su despacho. Una unidad de operaciones de la red identifica una cantidad inusual de tráfico que sale de su base dirigido a direcciones en otro país. La unidad notifica al Centro de Operaciones 624, incluyendo el personal de la Oficina de la Fuerza Aérea de Investigaciones Especiales, y el centro inicia esfuerzos de mando y control (C2) y ejecución de la ley para tratar el suceso. Se envían expertos forenses ciberespaciales para revisar la situación, no solamente localizando los equipos

“infectados” sino determinando también cómo el adversario accedió al sistema de la Fuerza Aérea. El C2 ciberespacial despacha personal de evaluación de riesgos de operaciones cibernéticas para estudiar la situación, determinar los datos exactos exfiltrados, y evaluar los daños. El equipo de respuesta de emergencia de la Fuerza Aérea (AFCERT) examina las computadoras y otros equipos de su base para rastrear los métodos de infiltración exactos, usándolos para desarrollar (y compartir) acciones defensivas específicas para la amenaza y filtrar cualquier táctica, técnica y procedimiento nuevos. El AFCERT recomienda parches a todas las computadoras de despacho de la Fuerza Aérea para combatir futuros intentos de emplear esta técnica; apoyará su base sobre una limpieza y protección adicionales de la red. Ahora que hemos descrito un ataque desde 15,000 metros, profundicemos en los sistemas y unidades armados que llevan a cabo estas misiones.

Sistema de armas de defensa del ciberespacio de la Fuerza Aérea

El sistema de armas de Defensa del Ciberespacio de la Fuerza Aérea (ACD) previene, detecta, responde y proporciona métodos científicos sobre las intrusiones en redes sin clasificar y clasificadas. El sistema de armas ACD, operado por el Grupo de Escuadras de Guerra de Redes (NWS) 33, ubicado en la Base Conjunta San Antonio–Lackland, Texas y el NWS 102 de la Guarda Nacional Aérea, ubicada en la Base de la Guarda Nacional Aérea Quonset, Rhode Island, apoya el AFCERT para satisfacer sus responsabilidades. Las tripulaciones para este sistema de armas consisten en un comandante de tripulación ciberespacial, un subcomandante de tripulación, un controlador de operaciones ciberespaciales y 33 analistas ciberespaciales, todos ellos apoyados por personal de misión adicional.

El sistema de armas ACD evolucionó a partir de AFCERT, que tiene la responsabilidad principal de coordinar los recursos técnicos del antiguo Centro de Guerra de Información de la Fuerza Aérea para evaluar, analizar y mitigar incidentes y vulnerabilidades de seguridad de computadoras. El sistema de armas ofrece un monitoreo y una defensa continuos de las redes sin clasificar y clasificadas de la Fuerza Aérea, que operan en cuatro áreas de disciplinas secundarias:

1. Prevención de incidentes: protege las redes de la Fuerza Aérea (AFNet) contra la lógica maliciosa nueva y existente; evalúa y mitiga las vulnerabilidades de software y equipos conocidos.
2. Detección de incidentes: lleva a cabo un monitoreo de AFNets clasificadas y sin clasificar; identifica e investiga actividades anómalas para determinar problemas y amenazas a redes; monitorea alertas de tiempo real generadas por sensores de redes; realiza una investigación detallada de tráfico histórico informado a través de sensores.
3. Respuesta de incidentes: determina la extensión de las intrusiones; desarrolla cursos de acción requeridos para mitigar amenazas; determina y ejecuta acciones de respuesta.
4. Informática forense: lleva a cabo un análisis detallado para determinar amenazas de incidentes identificados y actividades sospechosas; evalúa daños; apoya el proceso de respuesta de incidentes, captura el impacto completo de diversas actividades; efectúa la ingeniería inversa el código para determinar el efecto en la red/sistema.

Sistema de armas de análisis de defensa ciberespacial

El sistema de armas de Análisis de Defensa Ciberespacial de la Fuerza Aérea (CDA) lleva a cabo operaciones ciberespaciales defensivas monitoreando, recopilando, analizando e informando sobre información sensible emitida por sistemas sin clasificar amigos, como redes de computadoras, teléfonos, correo electrónico y sitios de web de la Fuerza Aérea de EE.UU. El CDA es vital para identificar divulgaciones de seguridad de operaciones. El sistema de armas es operado por tres unidades de servicio activo (NWS 68; NWS 352; y NWS 352, Destacamento 1) y dos unidades de Reserva de la Fuerza Aérea (Vuelo de Combate de Redes 860 y Vuelo de Combate de Redes 960) ubicado en la Base Conjunta San Antonio–Lackland, Texas; Base Conjunta del Campo de Aviación Pearl Harbor–Hickam, Hawaii; Base Aérea Ramstein, Alemania; y Base de

la Fuerza Aérea Offutt, Nebraska. Las tripulaciones de este sistema de armas constan de un controlador de operaciones ciberespaciales y tres analistas de defensa ciberespacial. Todas las tripulaciones de misiones reciben apoyo de personal de misiones adicionales.

Las dos variantes del sistema de armas de CDA están diseñadas para monitorear, recopilar, analizar e informar sobre información oficial de la Fuerza Aérea transmitida por medio de telecomunicaciones no seguras a fin de determinar si cualquiera de ellas es sensible o clasificada. El sistema informa sobre concesiones a comandantes de operaciones, monitores de seguridad de operaciones, u otros, según sea necesario, para determinar efectos potenciales y ajustes de operaciones. La segunda variante proporciona funcionalidad adicional para llevar a cabo la evaluación de daños de información basándose en intrusiones de la red, junto con una evaluación de sitios web sin clasificar de la Fuerza Aérea. Solamente el NWS 68 opera la segunda variante.

El sistema de armas de CDA suministra monitoreo y evaluación en seis áreas de disciplinas secundarias:

1. Telefonía: monitorea y evalúa las redes de voz sin clasificar de la Fuerza Aérea.
2. Frecuencia de radio: monitorea y evalúa las comunicaciones de la Fuerza Aérea dentro de las bandas de frecuencia VHF, UHF, FM, HF y SHF (teléfonos móviles, radios móviles terrestres y redes de área local inalámbricas).
3. Correo electrónico: monitorea y evalúa el tráfico de correo electrónico sin clasificar de la Fuerza Aérea a través de AFNet.
4. Capacidades basadas en Internet: monitorea y evaluar información que se origina dentro de la AFNet que se anuncia en capacidades basadas en Internet accesibles públicamente que no son propiedad, no están operadas o no están controladas por el Departamento de Defensa (DOD) o el gobierno federal.
5. Evaluación de riesgos de operación ciberespacial (encontrada dentro de la segunda variante operada por el NWS 68): evalúa datos comprometidos por intrusiones de las AFNets con el objetivo de determinar el efecto asociado en operaciones resultantes de esa pérdida de datos.
6. Evaluación de riesgos de la web (encontrados dentro de la segunda variante operada por el NWS 68): evalúa información anunciada en sitios web públicos y privados sin clasificar que son propiedad o están arrendados u operados por la Fuerza Aérea para minimizar su explotación por parte de un adversario, disminuyendo cualquier efecto adverso en las operaciones de la Fuerza Aérea y conjuntas.

Evaluación de Vulnerabilidad del Ciberespacio/Sistemas de Armas Hunter

El sistema de Evaluación de Vulnerabilidad del Ciberespacio (CVA)/sistema de armas Hunter de la Fuerza Aérea ejecuta evaluaciones de vulnerabilidad, cumplimiento, defensa y no técnicas, revisiones de las mejores prácticas, pruebas de penetración y misiones de búsqueda en redes y sistemas de la Fuerza Aérea y del Departamento de Defensa. Las operaciones de búsqueda caracterizan y después eliminan amenazas con el fin de controlar la misión. Este sistema de armas puede realizar salidas defensivas en todo el mundo por medio de un acceso remoto o en el sitio. El sistema de armas de CVA/Hunter es operado por una unidad de servicio activa, el Grupo de Escuadras de Operaciones de Información 92, ubicado en la Base Conjunta San Antonio–Lackland, Texas, y una unidad de Guardia, la NWS 262, ubicada en la Base Conjunta Lewis-McChord, Washington. Además, hay dos unidades de Guardia que se están transformando para esta misión: el Grupo de Escuadrones de Operaciones de Información 143 ubicado en Camp Murray, Washington, y el NWS 261 ubicado en la Estación de la Guardia Nacional de Aire de Sepulveda, California. Las tripulaciones para este sistema de armas consisten en un comandante de tripulación ciberespacial, uno a cuatro operadores ciberespaciales, y uno a cuatro analistas ciberespaciales. El personal de misiones adicional apoya todas las tripulaciones de misiones. Desarrollado

por el anterior Centro de Operaciones de Información de la Fuerza Aérea, el sistema de armas de CVA/búsqueda se desplegó en el Ala de Operaciones de Información 688 en 2009.

Históricamente, las evaluaciones de vulnerabilidad demostraron ser importantes para el control de la misión durante las Operaciones Libertad Duradera y Libertad Iraquí. Las CVA siguen proporcionando esta capacidad vital. Además, ahora sirven como la primera fase de las operaciones de búsqueda. La misión de búsqueda se desarrolló a partir del cambio de estrategia ciberespacial defensiva desde “intento de defender toda la red” hasta “control de la misión en la red”, ofreciendo una capacidad de habilitación para implementar una estrategia robusta de defensa profunda. Los prototipos del sistema de armas de CVA/búsqueda han participado en operaciones del mundo real desde noviembre de 2010. El sistema de armas logró una capacidad operacional inicial en junio de 2013.

El sistema CVA/Hunter, diseñado para identificar vulnerabilidades, da a los comandantes una evaluación completa del riesgo de vulnerabilidades existentes en redes de misiones críticas. Está funcionalmente dividida en una plataforma móvil usada por los operadores para llevar a cabo misiones ya sea en el sitio o en posición remota, una plataforma de sensores desplegable para reunir y analizar datos, y una plataforma de guarnición que proporciona la conectividad necesaria para operaciones remotas así como capacidades de análisis avanzados, pruebas, adiestramiento y archivado. Específicamente, la misión de búsqueda se concentra en encontrar, arreglar, hacer el seguimiento, seleccionar blancos, enfrentarse y evaluar la amenaza persistente avanzada.

Durante los enfrentamientos activos, el sistema de armas de CVA/Hunter, junto con otras fuerzas de defensa de redes amigas, proporciona a los comandantes ciberespaciales de la Veinticuatro Fuerza Aérea/Fuerzas Aéreas y comandantes combatientes una capacidad de protección de precisión móvil para identificar, perseguir y mitigar amenazas ciberespaciales. Puede armarse con una variedad de cargas útiles de capacidad modular optimizadas para misiones defensivas específicas y diseñadas para producir efectos específicos en el ciberespacio. Cada tripulación de CVA/Hunter puede llevar a cabo una variedad de evaluaciones, incluidas las pruebas de vulnerabilidad, cumplimiento y penetración, junto con análisis y caracterización de datos derivados de estas evaluaciones. Las cargas útiles del sistema de armas consisten en equipos y software listos para su uso comerciales y gubernamentales, incluidos los sistemas operativos Linux y Windows cargados con herramientas de evaluación de vulnerabilidad especializadas.

Sistema de armas de control de la red interna de la Fuerza Aérea

El sistema de armas de Control de la Red Interna de la Fuerza Aérea (AFINC) es el límite de máximo nivel y punto de entrada en la red de información de la Fuerza Aérea, que controla el flujo de todo el tráfico externo y entre bases a través de portales estándar gestionados centralmente. El sistema de armas AFINC consta de 16 conjuntos de portales y dos conjuntos de gestión integrados. El AFINC, operado por el Grupo de Escuadras de Operaciones de Redes (NOS) 26 ubicado en Gunter Annex, Montgomery, Alabama, tiene tripulaciones que consisten en un comandante de tripulación, un subcomandante de tripulación, un jefe de tripulación de operaciones ciberespaciales, dos controladores de operaciones, dos operadores ciberespaciales y tres controladores de sucesos, todos ellos apoyados por el personal de misiones adicional.

El sistema de armas AFINC reemplaza y consolida distintas AFNets gestionadas regionalmente en un punto de acceso gestionado centralmente para tráfico a través de la red de información de la Fuerza Aérea. Suministra servicios centrados en la red, habilita servicios básicos y ofrece una mayor agilidad para tomar medidas defensivas a través de la red. El AFINC integra operaciones de la red y defensa mediante cuatro áreas de disciplinas secundarias:

1. Defensa en profundidad: suministra un método en capas en toda la empresa integrando el portal y los dispositivos limitadores para proporcionar una mayor resistencia de redes y control de las misiones.

2. Defensa proactiva: lleva a cabo un monitoreo continuo del tráfico de AFNet para tiempo de respuesta, capacidad de producción y rendimiento a fin de asegurar un suministro oportuno de información crítica.

3. Normalización de redes: crea y mantiene normas y políticas para proteger redes, sistemas y bases de datos; reduce la complejidad de mantenimiento, el tiempo de inactividad, los costos y los requisitos de adiestramiento.

4. Conocimientos de la situación: suministra flujo de datos de la red, pautas de tráfico, índices de utilización e investigación detallada de tráfico histórico para la resolución de anomalías.

Sistema de armas del sistema de seguridad y control ciberespacial de la Fuerza Aérea

El sistema de armas del Sistema de Seguridad y Control Ciberespacial (CSCS) de la Fuerza Aérea proporciona funciones de operaciones y gestión de redes continuas, habilitando servicios de empresa clave dentro de las redes sin clasificar y clasificadas de la Fuerza Aérea. También apoya operaciones defensivas dentro de esas AFNets. El CSCS es operado por dos NOS de servicio activo, un Grupo de Escuadrones de Seguridad de Operaciones de Redes de la Guardia Nacional del Aire, y dos NOS asociados de comando de reserva de la Fuerza Aérea alineados con los grupos de escuadrones de servicio activo. Los NOS 83 y NOS 860 están ubicados en la Base de la Fuerza Aérea Langley, Virginia; los NOS 561 y NOS 960 de la Base de la Fuerza Aérea Peterson, Colorado; y el Grupo de Escuadrones de Seguridad de Operaciones de Redes 299 de la Base de la Fuerza Aérea McConnell, Kansas. Las tripulaciones de este sistema de armas consisten en un comandante de tripulación ciberespacial, un controlador de operaciones ciberespaciales y una tripulación de vuelo de operaciones (llevando a cabo funciones de límites, infraestructura, defensa de redes, foco de redes y vulnerabilidad-gestión), y una unidad de servicio de empresas (suministro de mensajes y colaboración, servicios de directorio y autenticación, gestión de almacenamiento y virtualización, y gestión de monitoreo). El personal de misiones adicional apoya a todas las tripulaciones de las misiones.

El CSCS resultó de una iniciativa operacional para consolidar numerosas redes principales específicas de mandos relacionadas con datos de bases de datos separadas en una red gestionada y controlada centralmente bajo tres centros de operaciones y seguridad de redes integradas. En 2007, la Fuerza Aérea estableció dos NOS de servicio activo para proporcionar estas funciones. El grupo de escuadrones de seguridad de operaciones de redes de la Guardia Nacional Aérea hace lo mismo para las bases y unidades de la Guardia.

El sistema de armas del CSCS realiza operaciones de redes y actividades de resolución de fallas diseñadas para mantener redes operacionales. Sus tripulaciones monitorean, evalúan y responden a sucesos de las redes de tiempo real; identifican y caracterizan actividades anómalas; y dan respuestas apropiadas cuando son dirigidos por comandancias superiores. El sistema apoya la filtración de tráfico de redes de tiempo real dentro y fuera de enclaves de nivel básico de la Fuerza Aérea y bloquea software sospechoso. Las tripulaciones del CSCS se coordinan continuamente con centros de redes de nivel básico y puntos de enfoque de comunicaciones para resolver temas de redes. Entre las capacidades clave adicionales se incluyen identificación y remedio de vulnerabilidades así como control y seguridad de tráfico de redes que entran y salen de enclaves de redes de nivel básico de la Fuerza Aérea. El CSCS ofrece también servicios de empresas de la Fuerza Aérea, incluidos mensajes y colaboración, almacenamiento y entornos controlados para disponer de sistemas basados en la red que apoyan las misiones de servicio.

Sistema de armas del sistema de misiones de mando y control ciberespaciales

El sistema de armas del Sistema de Misiones de Mando y Control Ciberespaciales (C3MS) habilita la misión de la Fuerza Aérea sincronizando otros sistemas de armas ciberespaciales del

servicio para producir efectos a nivel de operaciones en apoyo de comandantes combatientes de todo el mundo. Proporciona C2 a nivel de operación y conocimientos situacionales de sistemas de fuerzas, redes y misiones ciberespaciales de la Fuerza Aérea, habilitando al comandante de la Veinticuatro Fuerza Aérea para desarrollar y diseminar estrategias y planes cibernéticos; el comandante puede ejecutar y evaluar después estos planes en apoyo de los combatientes de la Fuerza Aérea y conjuntos. El sistema de armas C3MS, operado por el Centro de Operaciones 624 de la Base Conjunta San Antonio–Lackland, Texas, tiene tripulaciones que consisten en un oficial de servicio activo, un suboficial de servicio superior, un oficial de guarda ciberespacial defensivo, un oficial de guarda ciberespacial ofensivo, un oficial de guarda de la red de información del Departamento de Defensa, tres controladores de operaciones ciberespaciales defensivas, tres controladores de operaciones ciberespaciales ofensivas, tres controladores de operaciones de redes de información del Departamento de Defensa, un planificador de efectos ciberespaciales, un estratega de operaciones ciberespaciales, un analista de inteligencia ciberespacial, un analista de evaluación de operaciones ciberespaciales y un analista de celdas de información de operaciones ciberespaciales. Todas las tripulaciones de las misiones están apoyadas por personal de misión adicional. El sistema de C3MS evolucionó desde el concepto, el personal y los equipos del centro de seguridad de operaciones de AFNet anterior. Con la activación del Mando Ciberespacial de EE.UU. y la Veinticuatro Fuerza Aérea, los líderes superiores reconocieron la necesidad de una capacidad C2 ciberespacial a nivel de operaciones.

El C3MS es el único sistema de armas de la Fuerza Aérea que ofrece unos conocimientos perpetuos y amplios, gestión y control de la parte del servicio del dominio ciberespacial. Asegura un acceso sin trabas, control de misiones y uso de redes y sistemas de procesamiento de información de combatientes conjuntos para llevar a cabo operaciones a nivel mundial. El sistema de armas tiene cinco subcomponentes principales:

1. Conocimientos situacionales: produce una imagen operacional común uniendo datos de varios sensores, bases de datos, sistemas de armas y otras fuentes para ganar y mantener los conocimientos de actividades amigas, neutrales y de amenazas que afectan a las fuerzas conjuntas y a la Fuerza Aérea.
2. Productos de inteligencia, vigilancia y reconocimiento (ISR): permiten la integración de indicaciones y advertencia ciberespaciales, análisis, y otros productos de inteligencia accionable en conocimientos situacionales generales, planificación y ejecución situacionales.
3. Planificación: se aprovecha de los conocimientos situacionales para desarrollar planes a largo y corto plazo, estrategia adaptada, cursos de acción; conforma la ejecución de operaciones ciberespaciales ofensivas, operaciones ciberespaciales defensivas, y operaciones de redes de información del Departamento de Defensa.
4. Ejecución: se aprovecha de planes para generar y hacer el seguimiento de varias órdenes de tareas ciberespaciales para emplear fuerzas asignadas y agregadas en apoyo de operaciones ciberespaciales ofensivas, operaciones ciberespaciales defensivas y operaciones de redes de información del DOD.
5. Integración con otros nódulos C2: integra los efectos cibernéticos generados por la Fuerza Aérea con centros de operaciones aéreas y espaciales (AOC), Mando Ciberespacial de EE.UU. y otros nódulos C2.

¿Por qué sistemas de armas ciberespaciales?

Si realmente deseamos tratar el ciberespacio como un dominio operacional que no sea diferente del aéreo, terrestre, marítimo o espacial, entonces nuestro pensamiento debe evolucionar desde comunicaciones como función de apoyo a ciberespacio como dominio de combate operacional. Para volar y luchar de forma efectiva y ganar en el ciberespacio, la Fuerza Aérea debe organizar, adiestrar y equipar debidamente a sus profesionales del ciberespacio. Durante mu-

chos años, la infraestructura y los sistemas de AFNet crecieron como consecuencia de que múltiples comunidades añadieron componentes para adaptar sus necesidades individuales, a menudo con fondos de fin de año. De modo similar, los componentes que forman parte ahora de estos seis sistemas no tenían un mando guía principal para articular requisitos operacionales y asegurar un adiestramiento normalizado así como la gestión y los recursos efectivos de ciclos de duración de equipos. Dicho método incoherente hizo que el control de la misión y la defensa de las misiones críticas de la Fuerza Aérea y conjuntas en el ciberespacio fuera casi imposible. La migración a la AFNet ha permitido que el servicio se dirija a grandes pasos hacia la culminación de la visión de casi dos décadas de puesta en operación y profesionalización de la red. AFSPC apoyó con entusiasmo el esfuerzo de identificar estos seis sistemas de armas y facilitar este movimiento a un método más disciplinado. La designación formal de estos sistemas ayuda a asegurar una gestión y una sustentación apropiadas de los ciclos de duración de los equipos. También acelera la evolución de los profesionales ciberespaciales de la Fuerza Aérea desde una mentalidad de comunicaciones o tecnología de información a una operacional repleta con un adiestramiento de capacitación para misiones, normas de gestión de fuerza para tripulaciones y programas de normalización y evaluación (donde sea apropiado) para normalizar las operaciones ciberespaciales, como en el caso de las operaciones espaciales y misiles. Además, los sistemas de armas formalmente designados deben ayudar al ciberespacio a recibir la dotación apropiada y los fondos de programación necesarios para asegurarse de que la Fuerza Aérea puede volar, combatir y ganar en el ciberespacio.

La estructura del Departamento de Defensa para la gestión y los recursos de superioridad aérea, espacial, terrestre y marítima se produce a través de sistemas de armas. La mejor forma de crear y controlar efectos en el dominio ciberespacial comprende el uso de la misma estructura de sistemas de armas para gestionar y asignar recursos de capacidades ciberespaciales. Los sistemas de armas ciberespaciales ofrecen una vía para que la Fuerza Aérea ponga en operación, normalice, y por último normalice en el ciberespacio, justo como lo hemos hecho con los otros dominios de combate. Se ha encargado a la Fuerza Aérea que asegure, opere y defienda su parte de las redes de información del Departamento de Defensa y que defienda las misiones de la Fuerza Aérea y conjunta en el dominio ciberespacial. Estos sistemas de armas ciberespaciales dan a la Fuerza Aérea una guía para seguir en las operaciones de normalización para culminar este objetivo.

La designación de los sistemas de armas ciberespaciales creó una línea de financiación de sustentación ciberespacial separada en el proceso general de sustentación de sistemas de armas de la Fuerza Aérea. Al normalizar el proceso de financiación, el servicio ha instituido una planificación y programación de financiación de sustentación a largo plazo apropiadas, permitiendo así un uso más efectivo y eficiente de estos recursos limitados, comparados con la ejecución no coordinada de fondos de fin de año en los que no se puede confiar—ideas clave para garantizar la gestión de configuración normalizada e interoperabilidad de todos los servicios (y, donde corresponda, conjunta). Ya estamos obteniendo estas ventajas mediante el despliegue de AFNet, donde la empresa de la Fuerza Aérea se ha hecho más fácil de defender y la experiencia del usuario sigue mejorando mediante una normalización continua.

Las ventajas de designar sistemas de armas ciberespaciales son similares a aquellas ganadas por sistemas de armas en otros dominios—es el mecanismo estándar de la Fuerza Aérea para organizar, adiestrar, equipar y presentar capacidades de misiones. La estructura del sistema de armas permite que el servicio gestione capacidades de operación en un método formalizado y asegura su normalización, sostenimiento y disponibilidad a los comandantes combatientes. Cuando el personal de AFSPC comparó los procesos de normalización de los dominios del aire y el espacio, encontraron que solo la designación del sistema de armas suministró el estado final deseado. Dichos sistemas tal vez no tengan los recursos ideales, pero ciertamente reciben mejor apoyo que sin designaciones.

Además, designando sistemas de armas ciberespaciales directamente apoya la función de AFSPC como integrador guía de funciones básicas ciberespaciales, permitiendo al comando cumplir con las responsabilidades indicadas en la Directiva de la Política de la Fuerza Aérea 10-9 y facilitar la normalización en las plataformas del ciberespacio.³ Designar estos sistemas de armas también es crítico para proporcionar a las unidades tácticas los recursos y el adiestramiento necesarios para operar en una capacidad normalizada. La base de la integración entre dominios radica en la capacidad de aprovecharse de capacidades de diferentes dominios para crear efectos exclusivos y decisivos—si se controlan de forma adecuada. Dichas designaciones apoyarán la evolución apropiada del dominio ciberespacial y su relación con los otros dominios operacionales—un punto críticamente importante porque en la guerra moderna, el ciberespacio interconecta todos los dominios. La elevación de las capacidades operacionales en el ciberespacio a esta norma permitirá a la Fuerza Aérea satisfacer la *Department of Defense Strategy for Operating in Cyberspace* (Estrategia para la operación en el ciberespacio del Departamento de Defensa), que asevera que el “Departamento de Defensa tratará el ciberespacio como un dominio operacional para organizar, adiestrar y equipar de modo que el Departamento de Defensa pueda aprovecharse completamente del potencial del ciberespacio”.⁴

Todos estos esfuerzos para normalizar y hacer operacional las operaciones y misiones ciberespaciales impulsan a la Fuerza Aérea hacia la estructura, las normas y los procesos del Entorno de Información Conjunta (JIE). Como el Departamento de Defensa, el Mando Ciberespacial de EE.UU., y los servicios implementan el JIE, también hacen frente a equipos de misiones ciberespaciales para apoyar requisitos nacionales, de mando combatiente y ciberespaciales específicos del servicio. La designación de estas capacidades como sistemas de armas permite a estos equipos apoyar mejor las misiones nacionales y conjuntas, a través, y desde el ciberespacio.

Retos exclusivos del dominio ciberespacial

Los dominios aéreo, terrestre, marítimo y espacial son áreas naturales—no tuvimos que construirlos, como hicimos con las herramientas para aprovecharnos de esos dominios. Aunque ninguno de los dominios naturales exige mantenimiento, el ciberespacio existe predominantemente dentro de los equipos y dispositivos designados, contruidos y configurados por seres humanos, que requieren mantenimiento constante a medida que los equipos se hacen antiguos o se desgastan. Además, la forma en que construimos el ciberespacio tiene un efecto directo en nuestra capacidad para operar y defender el dominio. Este aspecto hace que el ciberespacio sea único en que su operación es justo tan importante como su defensa. Debemos alimentar y cuidar constantemente el dominio así como innovar para ir por delante, preferiblemente, impulsar la curva tecnológica.

La defensa del ciberespacio también presenta sus propios retos ya que un adversario puede lanzar un ciberataque virtualmente sin advertencia desde cualquier lugar del mundo. En el caso de los misiles balísticos intercontinentales, al menos tenemos sensores que detectan el lanzamiento; así pues, dependiendo del lugar del lanzamiento, nuestras fuerzas disponen de cierta advertencia ante la que responder. En el ciberespacio, los ataques pueden producirse sin advertencia o tiempo para crear y ejecutar respuestas. La Fuerza Aérea debe desarrollar capacidades para detectar dichos ataques, impedirlos si es posible, y responder de forma acorde si es necesario, así como lo hace en los demás dominios de combate. Debemos desarrollar también las herramientas para aprovechar el ciberespacio para nuestro propio beneficio. En realidad, tal vez no podamos defender nuestras redes completamente—para hacer eso probablemente se requeriría tanta seguridad que perderíamos los beneficios multiplicadores de fuerza que ofrece el ciberespacio a todas nuestras misiones. Si mantenemos fuera a todos los adversarios, lo más probable es que nos mantengamos bloqueados dentro. La clave radica en encontrar un equilibrio de

modo que defendamos efectivamente nuestras redes y las misiones que se basan en ellas del ataque pero aprovechemos el ciberespacio por el beneficio que ofrece a esas mismas misiones.

Además, el ciberespacio es crítico para las operaciones de la Fuerza Aérea y conjuntas en los otros dominios de combate. Prácticamente todo lo que hacemos en la guerra estos días radica en el ciberespacio, ya sea proporcionar telemetría a satélites y misiles o controlar el Blue Force Tracking (sistema de GPS que suministra información de ubicación de fuerzas amigas) en Afganistán—dependemos del dominio ciberespacial para ejecutar operaciones en los demás dominios.

La designación de sistemas de armas ciberespaciales requiere una tremenda dedicación de recursos para cumplir con las normas de sistemas de armas aéreas y espaciales. La operación según esta marca de referencia superior requiere la financiación y dotación correspondientes que el dominio ciberespacial recibido como una simple función de apoyo de tecnologías de comunicación o información. Sin embargo, no poder cumplir con estos compromisos podría ser devastador para las futuras operaciones en todos los demás dominios. La puesta en operación del ciberespacio es más que una forma justa en que el AFSPC organiza, adiestra y equipa debidamente las fuerzas ciberespaciales—es la evolución lógica del ciberespacio a un verdadero dominio de combate y un habilitador crítico de las demás operaciones de combate.

Caso práctico del centro de operaciones aéreas y espaciales

Un caso práctico escrito por el Teniente Coronel Jennifer Hlavaty resalta los puntos examinados arriba. A fines de los 90, la Fuerza Aérea designó el Falconer AOC como un sistema de armas con poca o ninguna adquisición formal, sustentación o rigor de requisitos para respaldarlo. Básicamente, el jefe de estado mayor simplemente lo puso en práctica sin detenerse en los detalles. La comunidad de operaciones se encontró retornando a los requisitos de la misma manera que lo hacemos hoy con nuestros sistemas ciberespaciales. Al declarar que el AOC era un sistema de armas, la Fuerza Aérea trató de normalizar lo que básicamente era una colección de equipos y personal que variaban de una fuerza aérea numerada a otra. Este pensamiento mantenía que un sistema de armas designado resultaría en un mejor adiestramiento de las tripulaciones de AOC, una mejor defensa del programa en el proceso de memorándums objetivo del programa, y cierta protección de la dotación de personal de la fuerza aérea numerada contra la apropiación para satisfacer alojamientos de AOC.

En realidad, la línea de financiación de AOC ha sufrido numerosos recortes, la referencia de equipos siempre ha sido problemática en términos de sustentación y modernización, y la dotación de AOC ha permanecido sujeta a varios simulacros de eficiencia, disminuyendo últimamente el rastro. Es razonable que muchos miembros de la comunidad de operaciones digan que la clasificación como sistema de armas no ha ayudado necesariamente al AOC.

No obstante, en opinión del Mando de Combate Aéreo, a pesar de los serios retos a los que nos hemos enfrentado durante la transición, el AOC está mejor hoy que hace 15 años, especialmente en términos de adiestrar a sus tripulaciones. Una unidad de adiestramiento formal especializada en Hurlburt Field, Florida, estableció un programa de registro, proporcionó una configuración rigurosa y proceso de gestión de cambios, y por último resultó en el reconocimiento, por parte de la comunidad de operaciones, que el AOC es la joya de la corona en el concepto de sistema de control aéreo C2 del comandante del componente aéreo de la fuerza conjunta. Además, la asignación a un período de servicio de AOC ya no está considerado como un acontecimiento de fin de carrera para oficiales homologados—cambio bastante grande desde la percepción de los años 90 cuando una asignación a un estado mayor de una fuerza aérea numerada o un AOC era ampliamente considerado como el golpe de gracia para la promoción en los campos profesionales homologados.

AFSPC no dejaría que las dificultades iniciales de la experiencia de AOC nos disuada de hacer avanzar el concepto de sistemas de armas ciberespaciales. Todo programa (aviones caza, bom-

barderos e ISR) se enfrentó a su buena parte de retos, pero sin un programa—algo con un nombre adosado—los sistemas ciberespaciales lucharían siempre por obtener pedacitos de dinero y dotaciones. A medida que integramos estos sistemas de armas ciberespaciales en la estructura de la Fuerza Aérea, quizás podemos aprender de los retos de establecer el sistema de armas de AOC y evitar los mismos errores y equivocaciones.

Pensamientos finales

A través del dominio del ciberespacio, los Estados Unidos explota a otros dominios de combate. Prácticamente toda la guerra se basa en estos días en el ciberespacio—todo desde comunicaciones, navegación y sincronización de precisión, advertencia de ataques, ISR y C2. La designación de sistemas de armas ciberespaciales ayudará a la Fuerza Aérea a garantizar el acceso al ciberespacio persistente y control de misiones para otros sistemas y dominios de armas críticos que se basan en el ciberespacio. Al hacer eso, el servicio se ha comprometido a que el ciberespacio recibirá la atención programática y presupuestaria necesaria para sostener las operaciones ciberespaciales, apoyar los equipos de misiones ciberespaciales e impulso hacia el JIE. Además, las operaciones ciberespaciales apoyadas por sistemas de armas básicos que ofrecen seguridad, rendimiento, flexibilidad y capacidad total mayores sin paralelo en un entorno menos normalizado. La puesta en operación del ciberespacio es más que simplemente una manera de que el AFSPC organice, adiestre y equipo debidamente el dominio ciberespacial—es la evolución lógica del ciberespacio hacia un verdadero dominio de combate y un habilitador crítico para los demás dominios. □

Notas

1. Publicación conjunta 1-02, Department of Defense Dictionary of Military and Associated Terms (Diccionario de términos militares y asociados del Departamento de Defensa), 8 de noviembre de 2010 (modificada hasta el 15 de junio de 2013), 303, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
2. Mandiant, APT1: Exposing One of China's Cyber Espionage Units (APT1: Exposición de una de las unidades de ciberespionaje de China) ([Washington, DC: Mandiant, 2013]), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
3. Directiva de la política de la Fuerza Aérea 10-9, Lead Command Designation and Responsibilities for Weapon Systems (Designación y responsabilidades del mando guía para sistemas de armas), 8 de marzo de 2007, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afpd10-9/afpd10-9.pdf.
4. Departamento de Defensa, Department of Defense Strategy for Operating in Cyberspace (Estrategia de operación en el ciberespacio del Departamento de Defensa) (Washington, DC: Departamento de Defensa, julio de 2011), 5, <http://www.defense.gov/news/d20110714cyber.pdf>. bio text.



El General de Brigada Robert J. Skinner, USAF (BS, Park College; MS, Oklahoma City University) es el Vicecomandante de las Fuerzas Aéreas Cibernéticas (Air Forces Cyber (AFCYBER)). Es el enlace principal y representante personal ante el Comando Cibernético de Estados Unidos y la Agencia de Seguridad Nacional, además de apoyar las actividades operacionales de las Fuerzas Aéreas Cibernéticas con OSD, DNI, CIA y otros participantes claves de la NCR cibernética. El General recibió su grado de oficial en 1989 y es egresado de la Escuela Superior para Oficiales de Escuadrón, la Escuela Superior de Comando y Estado Mayor, la Escuela Superior de Guerra de la Fuerza Aérea y el Colegio Industrial de las Fuerzas Armadas. Entre los logros en su carrera se encuentran comandos de Grupo y Ala, múltiples comandos de escuadrón, una variedad de cargos en comunicaciones tácticas y fijas, y asignaciones de plana mayor en el Estado Mayor Conjunto, Estado Mayor de la Fuerza Aérea y en una Fuerza Aérea Numerada. Antes de ocupar su puesto actual, el General Skinner se desempeñó en calidad de Inspector General en el Cuartel General del Comando Espacial de la Fuerza Aérea, Base Aérea Peterson, Colorado. En esta capacidad, estuvo al mando de 70 personas, tres direcciones, que constaban de cinco ramas a cargo de evaluar el apresto de más de 300 unidades cibernéticas y espaciales del Comando Espacial de la Fuerza Aérea ubicadas en más de cien lugares a nivel mundial.