# La garantía de la misión mediante la defensa cibernética integrada

Coronel William D. Bryant, USAF

Los adversarios impugnan cada vez más la capacidad de la Fuerza Aérea de Estados Unidos de lograr sus misiones en y a través del ámbito ciberespacial. Aunque diferentes comunidades dentro del servicio se enfocan en diversos métodos para un marco de defensa cibernética, la mejor manera de garantizar las misiones básicas de la Fuerza Aérea es a través de una combinación de defensa a profundidad, resistencia y defensa activa. Cada método es necesario, ninguno es suficiente, y el servicio debe combinarlos en un conjunto armonioso para lograr una eficacia máxima.

Las misiones esenciales de la Fuerza Aérea dependen en gran medida de la libertad de acción dentro del ámbito ciberespacial. Lamentablemente, la mayoría de los sistemas de armamento y misiones que se emplean en la actualidad las diseñamos para un mundo antes del surgimiento de la *Internet*. La suposición implícita fue que nuestros sistemas funcionarían en un entorno ciberespacial fundamentalmente permisivo y que la mayor amenaza sería la inteligencia de señales del enemigo.[1] La Fuerza Aérea diseñó muchos de sus sistemas hace décadas, por lo tanto no es sorprendente que nadie pudo predecir el crecimiento explosivo y la importancia del ámbito ciberespacial. Cuando los arquitectos del sistema consideraron algún tipo de seguridad en la informática para los sistemas de armamento, los ingenieros normalmente dieron por sentado que las defensas fronterizas de la red bloquearían a los adversarios de manera que el entorno visto por estos sistemas de armamento se mantendría permisivo y protegido dentro de las defensas de la red.

Estas suposiciones implícitas han demostrado ser dramáticamente falsas. El avance de los ataques cibernéticos aumenta a diario a lo largo de los sectores militares, gubernamentales y civiles. Los sistemas cibernéticos físicos, aquellos que incluyen componentes físicos y cibernéticos, ya no son seguros —lo atestiguan los ataques exitosos de los sistemas de control y vehículos industriales.[2] Estas tendencias se comprenden bien y son obvias. Convirtiendo la situación en peligrosa se encuentra el hecho de que nuestros adversarios también entienden nuestra vulnerabilidad ante estos tipos de ataques y los recalcan en su doctrina oficial publicada.[3] De la misma manera que nuestros adversarios han llegado a pensar diferente acerca de la guerra en el ciberespacio, nosotros también debemos ajustar nuestra perspectiva.

La presencia de un enemigo que puede maniobrar dentro del ámbito ciberespacial requiere un método básicamente diferente que va más allá de las defensas estáticas basadas en la tecnología de la informática (IT, por sus siglas en inglés). Contemplar el ciberespacio como un ámbito de guerra nos ayuda a comprender la razón de que ello sea así. Carl von Clausewitz, el famoso teórico de la guerra, consideraba la guerra como dos luchadores, cada uno tratando de vencer al otro mientras que constantemente se ajustaban y reaccionaban a los movimientos más sutiles de su adversario.[4] Los métodos estáticos que no tratan lo que el enemigo está haciendo fracasarán porque éste reaccionará a lo que hemos hecho para anular su efecto.[5] La seguridad de la misión en y a través del ciberespacio no es básicamente un problema de IT sino un problema de la misión que requiere un enfoque en la misión y métodos que van más allá de lo que hemos llegado a pensar como seguridad cibernética tradicional. Parte de esta perspectiva es captar que el espacio cibernético llega mucho más allá que el IT tradicional y los sistemas ciber-físicos en los cuales dependemos.

## Sistemas ciber-físicos

Todos los sistemas modernos existen simultáneamente tanto en el ámbito físico como en el ciberespacial. Por ejemplo, abrir paneles en una aeronave de combate moderna revelará una gran cantidad de cajas electrónicas conectadas por cables. Por lo general, esas cajas no utilizan el protocolo de control de transmisión (TCP, por sus siglas en inglés) estándar/el protocolo de *Internet* (IP, por sus siglas en inglés) del protocolo de la red; más bien, pasan información a lo largo de canales de datos a otras cajas electrónicas, evidentemente correspondiendo a la definición de espacio cibernético mencionada en la Publicación Conjunta 3-12 (R), *Operaciones en el Espacio Cibernético*.[6] Tal como se destaca detalladamente más adelante, cualquier defensor que se queda tranquilo al saber que esas cajas electrónicas no están conectadas directamente a la Internet sino que están "separadas físicamente" debería pensarlo de nuevo. Él o ella debe percatarse que en casi todos los casos, esos sistemas están en realidad conectados a todo mediante varios grados de separación que los agresores han demostrado la capacidad de saltar mediante numerosos métodos.[7]

En vista de que sistemas de armamento, tales como los buques y las aeronaves, dependen tanto en el ciberespacio, las acciones dentro del ámbito ciberespacial afectan directamente a los sistemas de combate en los ámbitos físicos. Los adversarios pueden atacar esos sistemas en el ciberespacio a través de numerosos puntos de acceso. Esencialmente, cualquier conexión física que transmite datos o cualquier antena con un procesador detrás de ella es una vía potencial para un agresor. Ejemplos obvios incluyen los sistemas de mantenimiento y de logística, radios definidos por el *software* y enlaces de datos y otros sistemas físicos cibernéticos que los operadores pueden conectar a plataformas, tales como cápsulas o armamento. Para complicar las cosas aún más, estas vulnerabilidades no son estáticas sino que cambian constantemente.

Cada actualización de *software*, cada capacidad nueva y cada pedazo innovador de equipo puede introducir vulnerabilidades nuevas. Los defensores no pueden sencillamente "arreglar"

un sistema y alejarse, esperando que el sistema o la capacidad permanezca "arreglado". Además, la plataforma del sistema de armamento en sí puede que esté completamente segura, pero el mantenimiento, el apoyo y los sistemas de logística puede que sean igual de importantes para lograr la misión. Los escuadrones de las aeronaves de combate más modernas sin combustible no son más que blancos sumamente costosos. Para aumentar la complejidad aún más tenemos el hecho de que muchas dependencias críticas de la misión caen fuera de las fronteras de la Fuerza Aérea en los sistemas comerciales tales como energía y transporte sobre los cuales el servicio tiene un control limitado o ningún control. En algunos contextos operacionales, las naciones aliadas operan esos sistemas con sus propias leyes y prioridades, tornando aún más difícil influenciar cómo esos países protegen sus sistemas en los cuales la Fuerza Aérea depende. En vista de que la gama de vulnerabilidades es tan abrumante, debemos comenzar a definir qué es lo más importante.

## Terreno cibernético clave

Para poder definir nuestro terreno cibernético clave, debemos tomar en cuenta ambos tipos de recursos ciberespaciales que estamos analizando al igual que el nivel de análisis.[8] Los tres tipos de recursos son el IT tradicional, la tecnología operacional y las plataformas. Entre los sistemas IT tradicionales se encuentra redes tales como la *Nonsecure Internet Protocol Router* [red de direccionamiento no secreto del protocolo *Internet* (NIPR, por sus siglas en inglés)] y la *Secure Internet Protocol Router* [red de direccionamiento secreto del protocolo Internet (SIPR, por sus siglas en inglés)] al igual que sistemas de armamento basados en IT, incluyendo el centro de operaciones aéreas y otros sistemas de personal y logística. La tecnología operacional tiene que ver con procesos físicos controlados por computadoras tales como los sistemas de control industriales u otros tipos de sistemas de control tales como automatización de edificios o calefacción, ventilación y aire acondicionado.[9] La última categoría es relativamente nueva en los círculos militares pero ha logrado una amplia aceptación en el mundo civil. La última categoría, las plataformas, incluyen tanto al avión de combate F-16 como un crucero *Aegis*. Los expertos en seguridad cibernética tienden a sentirse muy cómodos y familiarizados con la IT tradicional, y están comenzando a concentrarse en la tecnología operacional pero aún no han comenzado realmente a descifrar cómo asegurar las plataformas.

No es suficiente sencillamente categorizar un tipo de recurso. Al definir un terreno cibernético clave, un analista también debe fijarse en tres niveles diferentes de análisis y tomar en cuenta el componente, el sistema y los niveles de la misión. Si nuestra prioridad es la seguridad de la misión, entonces tendremos que cambiar nuestro análisis por encima del nivel del componente, a través del nivel del sistema y por último al nivel de la misión. Inclusive una misión relativamente sencilla tal como contra-aire defensivo es sumamente compleja al nivel de misión cuando uno analiza los nodos y las interdependencias. Una aeronave de combate debe estar en la estación pero también debe contar con el armamento. ¿De dónde proviene ese armamento? ¿Cuáles sistemas son necesarios para transportarlos y cargarlos? ¿Están esos sistemas protegidos de un ataque cibernético? Cada pregunta genera más preguntas; los dueños de la misión y las analistas tendrán que trabajar juntos para determinar cuáles son los recursos más esenciales que garantizarán el éxito de la misión. Una vez que los analistas han completado su análisis de la misión, los líderes superiores tendrán que definir cuáles misiones son las más importantes para entonces decidir cómo van a distribuir los recursos entre ellas. ¿Qué es más importante —la superioridad aérea y espacial o la movilidad global rápida? ¿Es el ataque global más importante que la inteligencia, vigilancia y reconocimiento? En vista de que la cifra de vulnerabilidades es tan amplia, tendremos que emplear cuidadosamente nuestros recursos limitados para un resultado máximo.

## Perspectivas diferentes

Inclusive después que dirijamos nuestros esfuerzos hacia las vulnerabilidades más significativas, aún hay un problema sustancial. Varias comunidades contemplan el ciberespacio a través de lentes diferentes, basándose en su cultura institucional y experiencia. Es un poco como la antigua fábula de múltiples ciegos examinando un elefante y llegar a diferentes conclusiones sobre qué es. Cada ciego está correcto acerca de su área particular del animal, pero ninguno comprende el panorama completo. La confusión en la terminología verdaderamente no ayuda porque "cibernético" significa cosas diferentes para personas diferentes.

Todos estos factores conducen a que comunidades diversas ofrezcan distintos métodos como "la" respuesta a la seguridad en la misión en y a través del ciberespacio. Las comunidades de IT tradicional favorecen utilizar la defensa en profundidad y ofrecer múltiples capas de defensas estáticas basadas en IT. Esas comunidades tienden a depender en el cumplimiento y la seguridad; algunas hasta igualan el cumplimiento con la seguridad, creyendo que si los evaluadores verifican todo de la lista de verificación correcta, entonces el sistema en cuestión está seguro. Las comunidades de adquisición tienden a adoptar una opinión diferente, prefiriendo crear resistencia en los sistemas en lugar de intentar reacondicionar la seguridad más adelante. Ellos crean sistemas resistentes y adaptables, y su mayor dificultad a menudo radica en encontrar el lenguaje de contrato correcto que obliga a los vendedores verdaderamente desarrollar la resistencia — algo que es notablemente difícil de definir. Las comunidades de las operaciones ciberespaciales optan un tercer y muy diferente punto de vista para proveer seguridad en la misión, recurriendo a la defensa activa mediante la vigilancia y respuesta continua a los ataques. Este énfasis en la maniobra del ciberespacio, que depende en operadores y herramientas de gama alta, puede ser extremadamente arduo de implementar fuera de las redes tradicionales basadas en TCP/IP.

Los tres métodos tienen gran valor; no son exclusivos sino que se complementan, y cualquier defensa robusta debe incluir a los tres —integrados para apoyarse entre sí. Dicha integración ofrece una ventaja competitiva sostenida que a nuestros adversarios les resultará difícil reproducir por las diferencias en la cultura. La Fuerza Aérea cuenta con décadas de experiencias en operar conjuntamente y en equipos con integrantes de muchos servicios y experiencias mientras que la mayoría de nuestros posibles opositores aún están acostumbrados a operar dentro de compartimentos verticales tradicionales del servicio. Cada tipo de defensa plantea preguntas fundamentalmente diferentes; requiere conjuntos de métodos, herramientas y destrezas completamente diferentes y ofrece capacidades fundamentales que no se encuentran en otros métodos.

## Defensa a profundidad

Sin una defensa a profundidad sólida, basada en IT básico, demasiados agresores traspasarían, derribarían inclusive los sistemas resistentes y abrumarían a los defensores. Los cortafuegos *(firewalls)* y las defensas basadas en IT puede que no detengan a los agresores de alto nivel, pero sí eliminan la mayoría de los ataques de bajo nivel y le permiten a los defensores concentrarse en los agresores de alto nivel que pasan. Este desgaste de la mayoría de los ataques es también esencial para la resistencia ya que reduce la cantidad de daños sostenidos que el método de resistencia debe superar para permitir que la misión continúe. La pregunta básica que se le plantea a la defensa a profundidad es, ¿cómo este método puede dificultar con éxito los ataques a mis sistemas?

Lo hace agregando capas de defensa, muy parecido a un castillo con paredes múltiples. Para tomar prestado un término de criptología, el factor trabajo (o sea, el esfuerzo invertido para penetrar las defensas) es quizás la manera más apropiada para medir la defensa a profundidad.[10] Colocar en fila 10 de los mismos *firewalls* con la misma vulnerabilidad no es tan útil como utilizar dos *firewalls* diferentes que requieran diversas técnicas y herramientas para aprovecharlas. La

mayoría de las defensas en esta área están basadas en la tecnología, incluyendo *firewalls*, sistemas de detección de intrusión y prevención, listas negras, listas blancas y muchas otras tecnologías y métodos.

Una buena defensa a profundidad consta de varios componentes. Las defensas fronterizas constituyen su capa exterior, manteniendo alejados los ataques de bajo nivel o *"script kiddie"*, llamados así porque los piratas informáticos *(hackers)* sin experiencia que utilizan herramientas o escrituras por lo regular los ejecutan. No es suficiente contar solamente con una o varias capas afuera de una red o sistema. Una vez que un agresor logra entrar, el defensor aún lo debe bloquear con barreras internas múltiples. Los defensores deben configurar esas barreras para evitar el movimiento lateral, elevación de privilegios y la exfiltración de datos confidenciales. La gestión de la vulnerabilidad a lo largo de organizaciones es también parte de una buena defensa a profundidad. Para eliminar grandes secciones de la superficie de ataque, los administradores y los arquitectos deben cerrar no tan solo las vulnerabilidades sino también cerrar procesos y aplicaciones innecesarias. Desde luego, es fácil hablar de reducir la superficie de ataque, pero hacerlo es muy complicado porque a menudo involucre eliminar la funcionalidad y la facilidad de uso. Por lo regular, todos esos componentes son más eficaces si los arquitectos del sistema los incorporan desde el principio o los "integran" en lugar de "agregarlos" después. Hacerlo exige el diseño de sistemas buenos y seguros que toman en cuenta la seguridad a lo largo del proceso del diseño y se fijan dentro y fuera del sistema en el entorno en el cual ese sistema probablemente funcionará. Comenzar en la fase del diseño es realmente muy tarde; en cambio, la ingeniería de sistemas debe comenzar en la fase de requerimientos. Lamentablemente, indistintamente de cuántas capas los defensores agreguen, la defensa a profundidad no siempre ha tenido éxito contra determinados agresores.

Aunque necesarias para cualquier defensa exitosa, las defensas estáticas no son suficientes; lo agresores dinámicos y determinados siempre encuentran la manera de penetrar sistemas específicos. Los sistemas modernos son excepcionales en hacer conexiones y por ende crear una superficie de ataque. La posible área de vulnerabilidad de incluso sistemas IT relativamente sencillos es vasta. Para sistemas críticos, una versión extrema de defensa a profundidad es un sistema con separación de aire en el cual los arquitectos no tan solo han protegido varios posibles vectores de ataque en el sistema, sino que también han tratado de eliminarlos aislando físicamente el sistema sin conexiones directas a sistemas menos confiables. Parece que este método fuese infalible, pero en práctica es extremadamente difícil de poner en práctica.

En la mayoría de los casos, esos sistemas no están verdaderamente separados de aire porque mantenerlos requiere conectar otros sistemas de mantenimiento para actualizarlos o cambiarlos. Rara vez los diseñadores actualizan y escriben *software* que siempre permanece dentro del sistema propietario único. Los administradores de sistema podrían pensar que sus sistemas están verdaderamente separados de aire, pero un análisis de los mismos por personal capacitado en informática forense, por lo regular demuestran lo contrario. Incluso si los administradores fuesen lo suficientemente cuidadosos de en realidad separar del aire un sistema sin fugas, en la mayoría de los casos esa acción limitaría dramáticamente la funcionalidad. Después de todo, la razón de ser de la mayoría de los sistemas es compartir y procesar datos. Puede que una computadora esté "segura" si está desconectada, enterrada a 100 pies de profundidad y envuelta en seis capas de cinta aislante —pero también es inútil.

Por último, cabe mencionar que un sistema cibernético físico necesita sus propias defensas bajo la defensa a profundidad. Dicho sistema debe contar con algunas defensas que no dependen de una red anfitriona particular; en una aeronave, por ejemplo, ese sistema es sumamente móvil y los operadores y los mantenedores puede que lo conecten a diferentes redes. Incluso si ese no es el caso, dar por sentado que 100 por ciento de la seguridad será provista por una defensa particular no es prudente. Los arquitectos de seguridad no tan solo deben planificar las

maneras de mantener alejados a los adversarios sino también deben diseñar el sistema de manera que funcione aun cuando el enemigo adentro.

## Resistencia

En vista de que ninguna defensa será perfecta, los sistemas deben poder funcionar y llevar a cabo sus misiones con un enemigo interrumpiendo y atacando con algún nivel de éxito. A estas alturas, la resistencia de la misión da un paso hacia adelante y le dificulta al enemigo llegar a cabo sus objetivos. El Comité de Control de Riesgos del Departamento de Seguridad Nacional define la resistencia como "la capacidad de adaptarse a condiciones que cambian y prepararse para soportar y recuperarse de la interrupción".[11] La resistencia permite una defensa alejada de la perfección que aún logra la misión, aun cuando es atacada en un entorno cibernético impugnado.

Los ingenieros de redes y sistemas deben planificar para el éxito del enemigo y esperarlo. Ellos deben evitar puntos de fracaso único y blancos fáciles que le permiten al adversario interrumpir fácilmente el éxito de la misión de una organización. Un sistema de misión debe ser flexible y poder deformarse bajo presión pero aún llevar a cabo su misión—algo muy parecido a un tallo de bambú en lugar de un roble rígido.[12] Es muy importante que la misión, no el sistema, continúe siendo el objetivo de la resistencia; la resistencia en el ciberespacio puede que radique completamente fuera del mismo. Las tácticas, técnicas y los procedimientos puede que sustituyan las defensas técnicas. Por ejemplo, si un adversario interrumpe un sistema de logística, pero los especialistas en logística en tierra utilizan lápices y portapapeles para descifrar como hacer llegar los abastos al lugar correcto, entonces un procedimiento de contingencia ha proporcionado la resistencia que no tuvo nada que ver con las defensas basadas en IT. Otro ejemplo: Si un enemigo ataca todas las bombas inteligentes de un escuadrón y las torna inoperables en el ciberespacio pero el escuadrón cambia a municiones no guiadas y de todas maneras destruye el blanco, entonces el escuadrón ha garantizado la misión a pesar del fracaso de algunos sistemas.

La resistencia de la misión está concebida para lograr la misión bajo un ataque—al igual que un buque de guerra continúa combatiendo después de haber sido atacado en numerosas ocasiones. Por supuesto, hay muchas maneras de implementar la resistencia técnica y procesal. Los diseñadores construyen buques de guerra con blindajes gruesos y compartimientos herméticos para reducir la posibilidad de daños catastróficos cuando los proyectiles del enemigo atacan. Los diseñadores pueden incluir características similares en sistemas IT y cibernéticos físicos resistentes.

Crear sistemas resistentes incluye varios métodos que los analistas pueden agrupar ampliamente como rutas, segmentación y diversidad de misiones múltiples. Las rutas de misiones múltiples le dificultan al enemigo evitar el logro de la misión. Por ejemplo, si un enemigo interrumpe el sistema crítico A, ¿hay un B que pueda reemplazar sus funciones? Las rutas de misiones múltiples no se refieren solamente a la redundancia; el sistema B puede ser un tipo de sistema completamente diferente o ningún sistema en lo absoluto si un procedimiento B reemplaza la función mediante algún método no basada en el sistema tal como el rastreo manual. Para poder crear rutas de misiones múltiples se necesita un cambio significativo de mentalidad alejado de la eficacia. Un sistema completamente eficaz no tiene redundancia o capacidades repetitivas "excesivas"; un sistema o proceso resistente debe contar con esas cosas para evitar un punto único de fallo. En un buque de guerra, las rutas de misiones múltiples son las diferentes maneras que los operadores pueden maniobrar el buque. El timón es el mecanismo principal, pero si falla o el enemigo lo destruye, el buque se puede maniobrar más o menos empleando un empuje diferencial en diferentes hélices. Las rutas de misiones múltiples son un buen comienzo pero solamente ofrecen resistencia robusta si los diseñadores las segmentan las unas de las otras.

Con la segmentación, los fallos deben contenerse y no afectar todo el sistema. En un buque de guerra, un método de segmentación obvio ocurre a través de compartimientos herméticos. Cuatro motores discretos no ofrecen resistencia robusta si un solo impacto puede inundar y deshabilitarlos todos. En el ámbito ciberespacial, los arquitectos crean la segmentación a través de infraestructura física separada y *hardware* al igual que defensas basadas en IT para evitar el movimiento lateral entre varios segmentos de red amigos. Un peligro en las tendencias IT actuales es la virtualización. El dueño de una misión puede que tenga 10 servidores separados pero no percatarse que en realidad todos ellos están en el mismo *hardware* físico. La virtualización tiene ventajas considerables para la resistencia, pero los arquitectos deben aplicarla de una manera que evite puntos de fallo únicos. Separar los sistemas mediante la segmentación es un paso importante; el último es garantizar que esos sistemas no compartan las mismas vulnerabilidades.

Utilizar un solo sistema operacional, tipo de *hardware* o aplicación produce un punto único de fallo que se puede extender a lo largo de una organización y presentarle a un agresor una oportunidad importante. El estratega militar Edward Luttwak destaca que con un enemigo pensante, "la homogeneidad se puede convertir fácilmente en una posible vulnerabilidad".[13] Para nuestro buque de guerra hipotético, las rutas de misión múltiples y la segmentación son por lo general suficientes porque un agresor no tiene una forma realista de derrotar a la vez toda una categoría de sistemas redundantes al mismo tiempo. Un enemigo debe destruir cada torreta por separado; él no puede destruirlas todas a la vez. En el ámbito ciberespacial, es posible deshabilitar cualquier cifra de los mismos sistemas empleando la misma vulnerabilidad que un enemigo difunde rápidamente a lo largo de los sistemas. Si una organización depende completamente de un solo navegador para hacer funcionar sus sistemas de logística, entonces una vulnerabilidad en ese navegador podría cerrar el acceso a todos esos sistemas de logística. Sería mejor si los diseñadores permitieran dos o tres navegadores diferentes que se puedan usar para tener acceso y manipular los datos. Por supuesto, tener demasiados diferentes tipos de aplicaciones o sistemas operativos es más comúnmente el problema en las organizaciones. Esa sobreabundancia introduce un mayor número de vulnerabilidades al sistema en general. Los arquitectos deben encontrar el equilibrio correcto con una pequeña cantidad de sistemas bien defendidos en lugar de puntos únicos de fallo o grandes cantidades de sistemas no seguros.

Estos métodos para lograr la resistencia serán costosos, por lo que los programas de adquisición no los pondrán en vigor hasta que los líderes superiores hagan que la resistencia sea una prioridad y la incorporen al proceso de adquisición. Una dificultad en lograr la resistencia no ha sido ni en la ingeniería ni en los retos de diseño sino en encontrar el idioma contractual que impulse a los vendedores a crear sistemas verdaderamente resistentes. Las oficinas de programas miden el éxito del mismo según el coste, horario y rendimiento. Mientras que esos sean los únicos componentes de una libreta de calificaciones de un programa, la seguridad de la misión continuará "por debajo de la línea de reducción" y sin financiación. Es posible que los programas puedan captar la garantía de la misión y la resistencia bajo la métrica de rendimiento, pero programas de adquisición anteriores no le han dado prioridad a esos factores bajo rendimiento. Para obligar esta priorización, los líderes superiores deben estar dispuestos a tomar decisiones difíciles y rehusarse a permitir que los programas sigan adelante a través de los objetivos a menos que hayan incorporado la seguridad de la misión y la resistencia. Hacerlo resultará sumamente problemático de implementar a causa de las presiones del proceso de adquisición, pero hay indicios de que algunos líderes superiores están comenzando a adoptar este método. Esos individuos ilustran que en la resistencia y la seguridad de la misión en el ciberespacio, las personas son importantes.

El componente más crítico de la resistencia y la seguridad de la misión en el espacio cibernético muy a menudo radica fuera del mismo —con el guerrero humano. Las personas son las que hacen que esto funcione. Este hecho se aplica de modo generalizado, desde los ingenieros diseñando sistemas hasta los operadores averiguando procedimientos alternativos en el campo. Fa-

cultar a esas personas a que mejoren la resistencia requiere reconocimiento por parte de los líderes superiores de la importancia de la garantía de la misión y los cambios culturales que facultan a nuestros hombres del aire a hacer la diferencia. Es absolutamente esencial que la Fuerza Aérea se aproveche del guerrero humano y habitualmente lleve a cabo entrenamiento en un entorno impugnado por la cibernética empleando equipos rojos agresivos que imitan a un enemigo haciendo maniobras. Muchos de esos ejercicios irán mal, y el daño colateral en sistemas que no son de ejercicio es un riesgo que se conoce. La Fuerza Aérea también deben aprender a encontrar y celebrar no a aquellos hombres del aire que obtienen una calificación de 100 por ciento en una prueba estandarizada basada en cumplimiento sino aquellos que descubren e implementan métodos creativos que mantienen la misión en marcha durante ejercicios e inspecciones exigentes. El servicio no tiene una oportunidad realista de crear la garantía de la misión sin habitualmente y con precisión llevar a cabo ejercicios en un entorno impugnado por la cibernética. Aunque la resistencia es crítica para operar con éxito dentro de ese entorno, otro componente de una defensa fuerte es una fuerza que activamente encuentra y reacciona ante las maniobras de un enemigo.

## Defensa activa

El último componente —la defensa activa— contribuye una manera de descubrir y responder a amenazas persistentes avanzadas. Los defensores deben conocer constantemente el espacio y patrullas de su misión, buscando pequeños indicios que los pueden guiar hacia un enemigo escondido. La defensa activa, una que busca encontrar y derrotar a un adversario sofisticado que maniobra, ocasiona problemas para un enemigo que intenta permanecer en los sistemas por un largo tiempo.

La defensa activa es un término cargado emocionalmente que a menudo se refiere a operaciones de ofensiva afuera de los sistemas de un defensor. Sin embargo, el tema de esta discusión se alinea con las medidas internas de defensiva de las operaciones ciberespaciales defensivas, que se definen en la Publicación Conjunta 3-12 (R) y permanecen dentro de los límites del sistema del defensor.[14] Las acciones de respuesta de las operaciones ciberespaciales defensivas, o las acciones defensivas que se toman fuera del sistema del defensor, son importantes pero no forman parte de esta discusión.[15] También resulta importante destacar que la defensa activa no siempre implica monitorear y maniobrar en tiempo real; puede que dependa de verificaciones periódicas para algunos tipos de sistemas para los cuales el monitoreo en tiempo real ni es práctico ni deseable. La defensa activa no es un concepto nuevo y los operadores ya la han puesto en práctica en varios sectores claves.

Las organizaciones que se anticipan al futuro, tales como bancos importantes, comprenden la defensa activa y han cambiado a un modelo de red de monitoreo de seguridad que incluyen defensores activos dentro de la red.[16] En la actualidad la Fuerza Aérea también lleva a cabo defensa activa robusta en sus propios sistemas IT tradicionales, como NIPR y SIPR. Establecer cómo extender la defensa activa en sistemas cibernéticos físicos es mucho más abrumador. A corto plazo, los defensores probablemente necesitarán proteger el equipo tradicional basado en IT que rodea y toca un sistema cibernético físico tal como la planificación de una misión basada en *Windows* o sistemas de mantenimiento para una aeronave en lugar de implementar el monitoreo en la plataforma en sí. En el futuro, a medida que los ingenieros diseñen y fabriquen sistemas cibernéticos físicos, será posible incorporar algunos elementos de defensa activa donde sea apropiado. No será apropiada en todos los casos.

Monitorear y responder dentro de un dispositivo basado en *Windows o Linux* es relativamente sencillo en comparación con intentar ejecutar la defensa activa en un sistema cibernético físico que ejecuta *software* patentado y exclusivo (por ejemplo el conjunto de aviónica de una aero-

nave). Uno de los mayores obstáculos es crear una fuerza laboral capaz de comprender la piratería de IT tradicional y los protocolos patentados que hacen funcionar la aviónica o los sistemas de control industrial. Algunos dispositivos físicos cibernéticos no pueden modernizarse fácilmente; tampoco pueden hacerse cargo de las exigencias cada vez mayores de procesamiento y transmisión de datos que son necesarias para la ejecutar la defensa activa. Otro aspecto a tomar en cuenta es la superficie de ataque adicional introducida por los sistemas de monitoreo. Algunas herramientas de red poderosas están ahora disponibles para el monitoreo y respuesta. La idea de un enemigo teniendo acceso a esas herramientas en una red amiga debe enviar escalofríos a los defensores de la red y motivarlos a que la defiendan vigorosamente. Una vez que los arquitectos mitiguen esos riesgos, la defensa activa incluirá varios componentes.

Para poder poner en vigor la defensa activa, los arquitectos deben crear tres componentes: fuerzas de maniobra, sensores y herramientas. El mayor reto radica en crear fuerzas de maniobra que estén capacitadas, equipadas y que puedan ejecutar con éxito la defensa activa. Destrezas técnicas profundas junto con la creatividad y flexibilidad tienen mucha demanda en todas partes, pero son exactamente lo que la Fuerza Aérea necesita para crear fuerzas de maniobra en el ámbito ciberespacial. El servicio también debe diseñar "híbridos" que no solamente conocen la pila de protocolos TCP/IP del IT tradicional sino también deben contar con un entendimiento profundo de la aviónica, los sistemas de control industrial u otros protocolos de sistemas de control que valoran el cumplimiento y la conformidad. La cultura del servicio está cambiando, pero debe hacerlo más rápido si queremos evitar alienar a algunos hombres del aire que pueden ser nuestras fuerzas de maniobra más potentes en el espacio cibernético. Encontrar, capacitar y mantener las que necesitamos es un comienzo, pero también debemos darles los sensores que necesitan para encontrar un enemigo oculto.

Un conjunto de sensores capaz es el segundo componente de la defensa activa. Las fuerzas de maniobra ciberespaciales deben poder encontrar un enemigo oculto siguiendo pistas y pruebas a lo largo de las redes. Los sistemas estándares para detectar la intrusión, que son parte de cualquier defensa competente a profundidad, son un punto de partida, pero los sensores que las fuerzas de maniobra necesitan tienen que ir más allá y tener más capacidad. Esta última trae consigo mayores requerimientos de capacitación para el personal que utiliza los sensores porque el riesgo de un resultado negativo aumenta si ellos no comprenden sus herramientas y los efectos que pueden generar en la red. Una sola exploración extremadamente agresiva puede poner de rodillas a una red empresarial. También cabe mencionar que por lo regular los sistemas basados en firmas no tendrán amenazas avanzadas y persistentes. Hace mucho tiempo que los actores avanzados en el ciberespacio han podido escribir códigos maliciosos que los exploradores actuales no podrán encontrar —amenazas en las que los defensores activos se deben concentrar.

El último componente es que después que las fuerzas de maniobra en el ciberespacio han localizado a un adversario ocultándose en sus sistemas, deben contar con las herramientas o armamento que les permitan derrotarle (o sea, evitar que cumpla con sus objetivos). La interrupción, negación y decepción son todos posibles métodos para los defensores, una vez que identifiquen a un enemigo.[17] Después de dicho descubrimiento, los defensores creativos tienen todo un universo de maneras creativas para aprovecharse del mismo. Además, no tienen que limitarse a un enfoque "micro" a cualquier código que el enemigo ha implantado. El uso del trabajo en red definido por el *software* permite los enfoques "macros" que tienen que ver con cambiar todo el entorno en formas que lo convierten hostil a los programas maliciosos del enemigo. También es posible para los defensores reaccionar sobre el nivel del sistema y priorizar lo que ellos protegen, de la misma manera que el cuerpo humano sacrificará extremidades al congelarse para mantener el alma viva. Todos estos métodos exigen diferentes conjuntos de herramientas que los defensores deben tener desarrolladas y listas para utilizarlas inmediatamente.

## Avanzando más allá de la teoría

Aun cuando el modelo teórico que se sugiere aquí esté correcto, significa muy poco a menos que la Fuerza Aérea pueda en realidad ponerlo en vigor de manera significativa por toda la organización. El primer paso es que varias comunidades comprendan que aunque su método preferido para garantizar la misión esté correcto, los otros métodos también están correctos y que los tres métodos deben trabajar juntos para un resultado máximo. Un paso importante fue la creación de la Fuerza de *Tarea Cyber Secure* por el jefe de estado mayor de la Fuerza Aérea con una orden de revisar la garantía de las cinco misiones básicas en y a través de toda la organización. En vista de que la fuerza de tarea fue un modelo temporal, el reto ahora radica en crear esa visión a nivel de organización en un nuevo conjunto de estructuras o un marco duradero. Este último incluirá elementos de las comunidades IT, adquisición y operaciones ciberespaciales unidas a través de un proceso de gobernabilidad y organización. Sin duda, esos cambios a nivel de cuartel general son importantes, pero un cambio cultural arrollador en toda la Fuerza Aérea es difícil e importante.

Una cultura ciberespacial auto sostenible y en evolución de individuos facultados que valoran el espacio cibernético y conocen los beneficios para facilitar la misión es el estado final deseado de nuestros hombres del aire con respecto al ámbito ciberespacial. Como parte de la fuerza de tarea, el Equipo de Garantía Cibernética analizó los problemas que afecta la cultural ciberespacial de todos los hombres del aire —líderes, proveedores de servicio, guerreros cibernéticos y usuarios. Algunas de sus recomendaciones tienen que ver con crecer y desarrollar una fuerza laboral ciberespacial, proveerle comunicaciones estratégicas sobre el espacio cibernético a la fuerza laboral, crear y poner en vigor mejor estrategia e innovación orientada al ciberespacio y reclutar y retener expertos en el ciberespacio.[18] Mover una cultura no es fácil y tomará tiempo. En un plazo más corto, podemos hacer algunos cambios en cómo utilizamos nuestros especialistas ciberespaciales.

Fortalecer la capacidad para ejecutar exitosamente la defensa activa en las misiones básicas involucrará cambiar algunos recursos. Podemos razonablemente dar por sentado que la Fuerza Aérea no recibirá una cantidad sustancial de nuevos especialistas cibernéticos en el entorno presupuestario actual. Si 100 hombres del aire expertos en el ciberespacio están en una base, ¿cómo los líderes de la base los van a utilizar? Ahora mismo casi todos ellos están haciendo trabajos IT creando y manteniendo redes; los comandantes tendrán que cambiar a algunos de ellos a la defensa activa de esas redes. En vista de que el volumen de trabajo en crear y mantener las redes no disminuirá, los líderes deben tercerizar más trabajo, cambiando el dinero de otras prioridades. Esas decisiones sobre los recursos serán muy difíciles para el futuro. En la actualidad, la Fuerza Aérea está preparando el terreno agresivamente para ese futuro ejecutando exploradores múltiples para experimentar y definir la mejor manera para que los profesionales ciberespaciales funcionen a nivel de ala. Los líderes deben volver a considerar las prioridades de la misión para proveer recursos adecuadamente. Una de las primeras cosas que necesitan hacer es identificar y captar el impacto de la misión de su terreno ciberespacial clave.

Para poder garantizar eficazmente sus misiones en el espacio cibernético, la Fuerza Aérea debe contar con un mejor entendimiento del enemigo y sus misiones. Es sumamente difícil recopilar inteligencia en cuanto a las capacidades e intenciones ciberespaciales de un adversario, pero los profesionales de inteligencia están aportando enfoque y esfuerzo adicional a este campo tan importante. En el lado de la misión, los exploradores a nivel de ala están comenzando sus programas analizando y desarrollando sus terrenos cibernéticos claves después del entrenamiento adecuado. La comunidad de adquisición también está buscando múltiples misiones para desarrollar el terreno ciberespacial clave a nivel de las aptitudes básicas de la Fuerza Aérea. Todos estos pasos iniciales exigen más trabajo y desarrollo que ayudará a aclarar en camino hacia una defensa mejor integrada de las misiones básicas del servicio en y a lo largo del espacio cibernético.

## Conclusiones

La mejor manera de defender eficazmente tanto los sistemas basados en IT como los sistemas físicos cibernéticos es a través de un método combinado que incluya defensa basada en IT a profundidad, resistencia y defensa activa de esos sistemas. Los sistemas que dependen del espacio cibernético son esenciales para el éxito de la misión para la Fuerza Aérea en el mundo moderno, y un solo método no ofrecerá la defensa más robusta posible.

La defensa a profundidad, que representa la defensa inicial, bloquea la mayoría de los ataques — particularmente los menos sofisticados. Sin defensas IT básicas y sólidas, demasiado ataques atravesarán para que los sistemas resistentes se encarguen de ellos. Sin una buena defensa a profundidad, la defensa activa también fracasará porque los defensores estarán abrumados y no podrán ni separar ni encontrar los agresores sofisticados en medio de la masa del ruido.

La resistencia ofrece seguridad manteniendo las misiones en funcionamiento a pesar de algún éxito por parte del enemigo. Evita que los adversarios cumplan con sus objetivos de atacar sistemas amigos. Ninguna defensa será completamente eficaz, entonces sin resistencia, la defensa a profundidad es necesaria para cumplir con un estándar imposible de captar y detener cada ataque en la frontera. La resistencia también les facilita a los defensores de poder encontrar a un enemigo oculto ya que ellos deben afrontar numerosos nodos y sistemas para tener un efecto; por lo tanto, el adversario se torna más "ruidoso" y más sencillo de localizar que si pudiese silenciosamente interrumpir un solo sistema escondido que crea un fracaso total de la misión.

La defensa activa encuentra y responde las fuerzas enemigas sofisticadas tales como amenazas avanzadas y persistentes. Esto incluye monitorear y responderles a los adversarios dentro de las redes amigas pero no extendiéndose más allá hacia redes neutrales o enemigas. Sin la defensa activa, los adversarios de alto nivel que se escurren a través de nuestra defensa a profundidad basada en IT tendrán tiempo ilimitado para analizar nuestros sistemas, descubrir nuestras medidas de resistencia y definir maneras de derribar inclusive los sistemas resistentes bien construidos. La defensa activa también ofrece oportunidades para confundir o interrumpir a un enemigo respondiendo creativamente a sus ataques y posiblemente falsificando los efectos que él produce.

Solamente si combinamos estos tres métodos podremos obtener una garantía de la misión robusta de las misiones básicas de la Fuerza Aérea en y a través del espacio cibernético. Cada comunidad desempeña un papel crítico y cada una depende de la puesta en vigor exitosa de las otras categorías de la defensa ciberespacial. Este método combinado le saca partido a nuestras fuerzas culturales y experiencias en la guerra conjunta y puede lograr una ventaja competitiva duradera para la Fuerza Aérea de Estados Unidos. ❑

**Notas**

1. Durante la Guerra Fría los ingenieros diseñaron muchos sistemas para evitar que un enemigo escuchara las comunicaciones; la criptografía era muy común para los sistemas bélicos. Lo inesperado fue que un enemigo pudiese emplear las comunicaciones para alterar el funcionamiento de plataformas tales como tanques, buques o aeronaves.

2. Para los automóviles, consultar a Stephen Checkoway et al., "*Comprehensive Experimental Analyses of Automotive Attack Surfaces*" (Análisis exhaustivo experimental de las superficies de ataque automotriz) (artículo presentado ante la Conferencia de Seguridad USENIX, San Francisco, 10–12 de agosto de 2011), 3–5, http://www.autosec.org/pubs/cars-usenixsec2011.pdf; o Andy Greenberg, "*Hackers Remotely Kill a Jeep on the Highway—with Me in It*" (Piratas informáticos destruyen un *Jeep* en la carretera — conmigo adentro), *Wired*, 21 de julio de 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. *Stuxnet* ofrece un famoso ejemplo de una bomba atacando sistemas de control industrial. Para un análisis a profundidad, ver Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (*Stuxnet* y el lanzamiento de la primera bomba digital en el mundo), (New York: Crown Publishers, [2014]).

3. Timothy L. Thomas, "*Nation-State Cyber Strategies: Examples from China and Russia*" (Estrategias cibernéticas de una nación estado: Ejemplos de China y Rusia), en *Cyberpower and National Security* (Poder cibernético y la seguridad nacional), editores Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (Washington, DC: National Defense University Press y Potomac Books, 2009), 465–88.

4. Carl von Clausewitz, *On War* (Sobre la guerra), editores y traductores Michael Howard y Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

5. Para una discusión de extensión considerable sobre cómo la respuesta e interacción por parte de adversarios crea la lógica paradójica de la estrategia, ver Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Estrategia: La lógica de la guerra y la paz), edición revisada y ampliada (Cambridge, MA: Belknap Press of Harvard University Press, 2003).

6. El Estado Mayor Conjunto de Estados Unidos ha definido el espacio cibernético como "un ámbito global dentro del entorno de la informática que consiste en la red interdependiente de infraestructuras de la tecnología de la informática y datos residentes, incluyendo la *Internet,* las redes de telecomunicaciones, los sistemas de computadoras y los procesadores y controladores integrados". *Joint Publication* (JP)_(Publicación Conjunta) 3-12 (R), *Cyberspace Operations* (Operaciones ciberespaciales), 5 de febrero de 2013, GL-4, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

7. *Stuxnet* es el mejor ejemplo conocido de un ataque cruzando una brecha aérea bien defendida. Además, hay muchos otros ejemplos. Ver P. W. Singer y Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Ciberseguridad y ciberguerra: Lo que todos deben saber) (New York: Oxford University Press, [2014]), 63; y Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain" (El ciberespacio no es un ámbito bélico) *I/S: A Journal of Law and Policy for the Information Society* 8 (I/S: Una revista de leyes y política para la sociedad de la informática), núm. 2 (Otoño 2012): 323–24.

8. En este párrafo, el Dr. William Young en la Universidad del Aire diseñó la metodología clave del análisis del terreno ciberespacial. Lo empleo aquí con su permiso.

9. "*Operational Technology* (OT) (Tecnología operacional)", Gartner, consultado el 8 de septiembre de 2016, http://www.gartner.com/it-glossary/operational-technology-ot.

10. Shon Harris, *CISSP All-in-One Exam Guide* (CISSP Guía Integral del Examen), 6ª Edición. (New York: McGraw Hill, 2013), 768.

11. *Department of Homeland Security* (Departamento de Seguridad Interna), *Risk Steering Committee* (Comité de Control de Riesgos), *DHS Risk Lexicon*, 2010 ed. (Washington, DC: Department of Homeland Security, Risk Steering Committee, septiembre de 2010), 26, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

12. Para una discusión más complete de este concepto, consultar Coronel (USAF) William D. Bryant, "*Resiliency in Future Cyber Combat*" (Resistencia en el combate cibernético del futuro), *Strategic Studies Quarterly* 9, núm. 4 (Invierno 2015): 87–107.

13. Luttwak, *Strategy*, 40.

14. JP 3-12 (R), *Cyberspace Operations*, II-2–II-3.

15. Ibid., II-3.

16. Richard Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (La práctica de la vigilancia en la seguridad de la red: Comprendiendo la detección de incidentes y respuestas), (San Francisco: No Starch Press, 2013), ubicación en *Kindle* 263, capítulo 1.

17. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (La conquista en el ciberespacio: Seguridad nacional y guerra de informática) (New York: Cambridge University Press, 2007), 79–84.

18. Departmento de la Fuerza Aérea, "*Task Force Cyber Secure (TFCS) Team Cyber Assure Out Brief / Way Ahead*" (Fuerza de Tarea *Cyber Secure* [TFCS. por sus siglas en inglés] Informe final del equipo *Cyber Assure /*Camino por recorrer) presentación (Washington, DC: Department of the Air Force, 1 June 2016); y Departamento de Defensa, *Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)* (Cultura de Ciberseguridad e Iniciativa de Cumplimiento del Departamento de Defensa), (Washington, DC: Department of Defense, septiembre de 2015), http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

**Coronel William D. Bryant, USAF** (USAFA; MA, American Military University; MA, George Washington University; MSS [Maestría en Sistemas Espaciales], Air Force Institute of Technology; MAAS [Maestría en el Arte y la Ciencia del Poderío Aéreo]; PhD, School of Advanced Air and Space Studies; MSS [Maestría en Estudios Estratégicos], Air War College) es subdirector de la Fuerza de Tarea de Seguridad Cibernética para la Oficina del Dominio de la Información y del Oficial en Jefe de Información, Oficina del Secretario de la Fuerza Aérea, Pentágono, Washington DC. Autor de *International Conflict and Cyberspace Superiority: Theory and Practice* (El conflicto internacional y la seguridad ciberespacial: Teoría y práctica) (Routledge, 2015), es un piloto de combate de carrera, estratega y planificador que se ha desempeñado en varias asignaciones operacionales y de estado mayor.