Es Hora de Defenderse: "Operacionalización" de la Defensa de Redes

Nicolás Adam Fraser
Teniente Coronel (USAF-Ret) Robert J. Kaufman III
Teniente Coronel (USAF-Ret) Mark R. Rydell*

LA DECISIÓN DE la Fuerza Aérea de activar la Vigésimocuarta Fuerza Aérea bajo el Comando Espacial de la Fuerza Aérea crea una oportunidad de escudriñar conceptos de guerra de redes existentes con el objetivo de asegurarnos de que las operaciones de guerra de redes están incluidas en la misión indicada de la Fuerza Aérea: "volar, combatir y vencer . . . en el aire, en el espacio y en el ciberespacio".[1] Dicha revisión completa incorporaría un número significativo de organizaciones dentro y fuera de la Fuerza Aérea, que incluirían debates de política, prioridades de financiación, personal y coordinación entre servicios, entre otras cosas. Este artículo no tiene como fin tratar todos los temas complejos que se presentan en las operaciones ciberespaciales; sino que examina el componente más visible de la guerra ciberespacial—la defensa de redes (NetD).

Desde 1992, la Fuerza Aérea ha monitoreado sus redes y ha respondido a los eventos maliciosos en las mismas. A medida que el servicio ha madurado su capacidad de comandar y controlar sus redes, algunos principios de operación han mezclado inintencionadamente la NetD y las operaciones de redes (NetOps). Este artículo propone nuevos conceptos de operaciones que obligarán a hacer una distinción clara entre la guerra de redes—particularmente la NetD—y las NetOps. La asignación de ciberobjetivos, el primer concepto propuesto, hace énfasis en la necesidad de encontrar, resolver el problema, hacer el seguimiento y seleccionar un adversario como objetivo de forma proactiva. Las operaciones de asignación de ciberobjetivos pueden asegurar que los sistemas críticos de la misión o incluso las trayectorias de las redes estén libres de adversarios. El segundo concepto, el ciberenfrentamiento, es un grupo de respuestas diseñadas específicamente para afectar a un intruso identificado. Los conceptos actuales de la NetD y la asignación de ciberobjetivos permiten operaciones de ciberenfrentamiento. Por último, debemos coordinar estrechamente las operaciones de asignación de objetivos y enfrentamiento con comandos combatientes (COCOM) y las operaciones de otras agencias nacionales. Tanto la asignación de ciberobjetivos como el ciberenfrentamiento inducen un contraste robusto entre el mantenimiento de la red y la defensa de la red. Como consecuencia de hacer dicha distinción y emplear los conceptos propuestos, las operaciones de la NetD deben hacerse más efectivas.

Puesta en escena del cambio

La Fuerza Aérea ha estado discriminando sus definiciones de NetOps y NetD, la primera proporcionando "servicios de red de información efectiva, eficiente, segura y fiable usados en procesos de comunicación e información críticos del Departamento de Defensa (DOD)

*Los tres autores trabajan en la Escuadra Aérea de Operaciones de Información 688 de la Base de la Fuerza Aérea de Lackland, Texas, el Sr. Fraser como jefe de la Rama de Ingeniería de Acceso de Redes, el Teniente Coronel Kaufman como director auxiliar del Grupo de Operaciones de Información 318 y el Teniente Coronel Rydell como consultor superior de Booz, Allen y Hamilton. Los tres desempeñaron períodos de servicio en el Equipo de Respuestas de Emergencia de Computadoras de la Fuerza Aérea.

y de la Fuerza Aérea" y la segunda "empleando . . . capacidades basadas en la red para defender información amiga residente o en transición por redes contra esfuerzos adversarios a fin de destruir, interrumpir, corromper o usurpar. La NetD puede considerarse como planificar, dirigir y ejecutar acciones para impedir actividades no autorizadas en la defensa de sistemas y redes de información de la Fuerza Aérea y para planificar, dirigir y ejecutar respuestas para recuperarse de la actividad no autorizada en caso de que ocurra".[2] El hecho de que la comunidad conjunta carezca de un término que describa lo que la Fuerza Aérea llama NetOps significa que considera que las NetOps son un subconjunto de la NetD o simplemente una función de mantenimiento que no necesita debatirse en una publicación de doctrina conjunta.[3] Debido a las diferencias entre las doctrinas conjunta y de la Fuerza Aérea, sugerimos versiones simplificadas de la NetD y de las NetOps de modo que el lector pueda reconocer inmediatamente las responsabilidades y prioridades de cada operación:

- **Operaciones de guerra de la red/NetD:** Operaciones que tratan de producir efectos deseados contra un adversario de forma táctica, operacional y estratégica. Estas operaciones, que requieren apoyo de planificación e inteligencia, pueden ser reactivas o proactivas. Y lo que es más importante, las operaciones de NetD consideran el descubrimiento de un adversario no sólo una amenaza sino una oportunidad para el enfrentamiento operacional.
- **NetOps:** operaciones en las que el mantenedor principalmente *actúa sobre la red* para proporcionar servicios de red fiables y seguros. En realidad un adversario que interrumpa las operaciones no es peor que una falla en los equipos, ya que el objetivo incluye mantener la disponibilidad y los requisitos de rendimiento. Así como podemos reemplazar equipos, para que también podamos reconstruir una computadora en peligro.

Sostenemos que la Fuerza Aérea no lleva a cabo realmente operaciones de NetD según se define arriba. Apoyamos esta aseveración examinando dos principios en los que se basa el núcleo del método actual del servicio a la NetD y que mantienen a la Fuerza Aérea reactiva, debilitando así su capacidad de defender la red de forma efectiva.

Principio 1: Detectar al adversario es de una importancia suprema

Este principio, los cimientos sobre los que hemos construido la mayoría de las NetD tradicionales, consume la mayor parte de los recursos de la NetD de la Fuerza Aérea. El servicio se basa en un monitoreo en tiempo real y hace énfasis en unos perímetros de la red intensificados para detectar la actividad del enemigo. No obstante, su motivación para hacer eso es de gran importancia. La Fuerza Aérea desea detectar al intruso o al atacante, no tomar medidas contra él sino encontrar y resolver un problema de seguridad. La situación es análoga a la manera en que un miembro de las fuerzas de seguridad de una patrulla de línea de vuelo responde a un evento sospechoso. Después de ver a un intruso entrar por un agujero de la cerca, él o ella enciende la linterna y apunta hacia el agujero y empieza a arreglarlo en vez de seguir y capturar al intruso. Actualmente, la Fuerza Aérea no distingue entre intrusiones refinadas y no refinadas, tratando todas las brechas por igual y respondiendo de una manera que protege y restablece la salud de la red. No se concentra en asegurar que podemos efectuar las misiones requeridas y seguir las NetOps a pesar de sufrir ataques del adversario.

Aunque es importante, la detección del adversario no es sólo la única manera de proteger una red. Los cambios rápidos y regulares de su configuración también protegerían y no requerirían la detección del adversario para producir resultados.[4] Además, no abogamos el fin de los esfuerzos de detección, algo crítico para las operaciones de NetD según la definimos, pero debe cambiar la motivación detrás de los esfuerzos de detección. Por último, concedemos que nuestras mejores defensas

perimétricas y metodologías de gestión de parches no disuaden ni obstaculizan a los adversarios complejos.[5] Aunque estas metodologías son útiles, debemos complementar nuestro método actual con uno dedicado a lograr efectos contra el adversario y asegurar el éxito de la misión.

Principio 2: Las operaciones de NetD tienen éxito cuando una computadora en peligro deja de estar en peligro

Este principio relega las operaciones de NetD a una función de mantenimiento dentro de la Fuerza Aérea, hacienda énfasis en la salud de la red a expensas de determinar el efecto del enemigo en misiones en curso o futuras. Además, raramente usamos una computadora en peligro para enfrentarnos al adversario. Además de localizar, analizar y arreglar computadoras en peligro, los operadores de NetD deben contender con el adversario, incluso en nuestras propias redes, concibiendo y ejecutando estrategias defensivas que le afecten además de asegurar la integridad de misiones de combate prioritarias.

Debido a este principio, probablemente más que al otro, debemos definir realmente la NetD actual como NetOps. Cuando se produce una intrusión y abrimos un "incidente", ¿cuándo lo cerramos? No cuando concluya una operación sino cuando consideremos que la computadora esté libre de intrusos y permitamos que se vuelva a unir a la red. ¿Se considera que esto es un éxito? No. Debemos medir el éxito por la eficacia de combate; en consecuencia, debemos tomar medidas en los niveles estratégicos, operacionales y tácticos para determinar si estamos alcanzando los objetivos de la NetD como disuadir al adversario para que no establezca ni emplee capacidades ofensivas contra los intereses de EE.UU.[6]

Un nuevo concepto

Proponemos corregir estos problemas estableciendo unidades de operación (de tamaños aún sin determinar) encargadas de afectar verdaderamente las operaciones del adversario que fijan como objetivos redes de la Fuerza Aérea y del DOD. Cierto, las unidades de la Vigésimocuarta Fuerza Aérea (incluida la Escuadra Aérea de Operaciones de Información 688 y la Escuadra Aérea de Guerra de Redes 67) son responsables de ejecutar la misión cibernética de la Fuerza Aérea; no obstante, ninguna unidad de la Vigésimocuarta Fuerza Aérea hace ahora lo que sugerimos abajo. Nuestros nuevos paradigmas requerirán la reconformación de unidades existentes y, posiblemente, la creación de otras nuevas.

La primera organización propuesta tendría la misión enfocada internamente de buscar al adversario en las redes de la Fuerza Aérea y del DOD. La segunda tendría la misión enfocada exteriormente de enfrentarle en esas redes. Aunque ambos colaborarían estrechamente (y con la misión establecida de monitoreo continuo de la red), se separarían por su dedicación a las misiones planificadas o "salidas" enlazadas a las necesidades de operación del comandante y terminadas después de completar la misión. A niveles estratégicos, las políticas apropiadas necesitan endosar estrategias proactivas de la NetD como asignación de objetivos y enfrentamiento. A continuación, al nivel de operaciones, debemos desarrollar planes para tratar a adversarios específicos y prescribir cursos de acción aprobados que permitan a los defensores de la red obtener unidad de esfuerzo, masa, sorpresa y puntualidad en el ciberespacio. Por último, al nivel táctico, debemos adiestrar y certificar a operadores en armas de NetD que puedan poner en peligro ataques o desbaratar intentos de acceder a las redes de la Fuerza Aérea. Estas organizaciones y planes permitirán a la Fuerza Aérea efectuar operaciones de NetD que busque, se enfrenten y actúen sobre los adversarios en el ciberespacio.

Asignación de ciberobjetivos

Está claro que los enemigos—específicamente los avanzados y persistentes—residen dentro de la red de la Fuerza Aérea. Los ataques incisivos, que persuaden a los usuarios a abrir un anexo malicioso o a hacer clic en un enlace con una página web maliciosa, rompen las defensas perimétricas sin dificultad. La facilidad

con la que un adversario puede acceder a las redes del DOD es superada solamente por la facilidad con la que puede navegar y maniobrar después de establecer "cabezas de playa" dentro de las redes de la Fuerza Aérea y del DOD, las cuales ofrecen una entrada en la información o sistemas de alto valor. La asignación cibernética, un método proactivo, puede identificar a los intrusos en nuestras redes usando "armas" de NetD de última tecnología que no estén localizadas permanentemente en la red de la Fuerza Aérea, junto con herramientas de seguridad perimétrica típicas. Llevaríamos a cabo operaciones con un objetivo específico en mente, localizar al adversario, y después influir, interrumpir o afectarle. Una operación no terminaría hasta que hubiéramos identificado al adversario y hubiéramos verificado subsiguientemente su ausencia, sea cual sea el factor de terminación. Estas operaciones también exigen una planificación y una ejecución propias debido a la enorme cantidad de datos legítimos en el ciberespacio, dentro del cual se esconde el adversario para hacer su trabajo.

Ciberenfrentamiento

La defensa siempre ha consistido en demorar, interrumpir, disuadir o negar los objetivos al enemigo. Sin embargo, si asumimos la imposibilidad de detener completamente al adversario, entonces debemos considerar formas de obstaculizar o explotar significativamente sus esfuerzos. (Por "explotar", queremos decir lograr efectos de segundo y tercer orden sobre su capacidad de tomar decisiones). El ciberenfrentamiento toma la decisión consciente de usar las redes del DOD como una trayectoria para llegar al adversario—una trayectoria para lograr objetivos defensivos.[7] Después de descubrir una computadora o una red en peligro, los operadores de la NetD dejarían de reconstruir simplemente el sistema pero usarían la inteligencia y quizás otra armas de NetD para identificar al intruso. A continuación, dependiendo del nivel de atribución y de los planes de operación existentes (OPLAN), llevarían a cabo operaciones tácticas contra el adversario, utilizando la computadora o la red en peligro como punto de partida.[8] Por ejemplo, durante una operación, el operador de la NetD podría pasar información inexacta de forma intencionada al enemigo o manipular datos exfiltrados, haciendo que no sea digna de confianza. Sea cual sea la técnica empleada, el operador trataría siempre de introducir la falta de fiabilidad, encarecería las intrusiones o influiría en las acciones del adversario. En consecuencia, los operadores deben planificar y coordinar estas "medidas de respuesta" con COCOM más grandes o estrategias a nivel nacional.[9] Además, deben eliminar los conflictos de estas clases de operaciones del monitoreo diario de los sensores de la red.

Como hemos dicho antes, el ciberenfrentamiento cubre un espectro de operaciones, no simplemente un ataque de la red. El enfrentamiento supone la incapacidad de los esfuerzos de detección y protección para defender la red de la forma debida. En vez de eso, adopta un método diferente, uno que no está limitado a la selección de cierta tecnología sino que se preocupa por las acciones necesarias para cumplir con los objetivos defensivos. Para ilustrar esto, durante un partido de fútbol americano, los jugadores ofensivos tratan de llegar a la zona de anotación, pero la defensa trata de detenerlos. Los defensas de fútbol americano tratan de impedir que el equipo contrario entre en la zona de anotación no sólo empleando una defensa profunda (con una línea defensiva fuerte, linebackers [defensas de línea] y safeties [últimos defensas]) sino también usando distintos esquemas defensivos para confundir al mariscal. Por ejemplo, un linebacker podría apresurar al mariscal mientras que otros dos se retrasarían en la cobertura—o el coordinador defensivo podría ordenar un ataque relámpago total. Sea cual sea el esquema, los buenos directores técnicos saben que no siempre pueden impedir que el ataque consiga puntos, pero pueden dificultar su tarea confundiendo a los jugadores contrarios, especialmente al mariscal.

Fijándonos en esta analogía, tendríamos que decir que el DOD actualmente se defiende sin tener que pensar nunca en confundir a los atacantes. No disponemos de distintos esquemas defensivos, ni preparamos planes que

afecten la planificación, ejecución, y, por último, el resultado de un encuentro con el enemigo. En vez de eso, nuestra defensa se ubica en el perímetro de la red, y esperamos que nadie se quede sin detectar.

La asignación de ciberobjetivos y el ciberenfrentamiento representan un cambio de paradigma significativo en la forma en que realizamos las operaciones de la NetD. Teniendo en cuenta los objetivos del OPLAN enfocados, podemos hacer que la NetD sea una forma más fuerte de combatir que el ataque de la red.[10] Ciertamente, el Ejército de EE.UU. ya ha observado esto en las operaciones defensivas más tradicionales.[11] Además, la NetD puede asumir una función más activa en la guerra de redes mientras se crea una distinción muy necesaria entre ella misma y las NetOps. Por último, estos nuevos conceptos apoyan el deseo del presidente de ir más allá del enjuiciamiento penal para responder de forma apropiada a los ataques cibernéticos.[12]

Una propuesta sencilla

La planificación y la preparación de operaciones militares a gran escala, como la invasión de Irak en 2003, requieren que los OPLAN de los COCOM sean encaminados a través de cada organización de NetD principal del servicio militar, permitiendo así que los defensores de la red implementen medidas para evitar que las redes del DOD se conviertan en objetivos del enemigo e impidan cualquier interrupción de la ejecución del OPLAN. Los requisitos proporcionados por los COCOM tratan normalmente de amenazas genéricas. Cuando comienzan las operaciones, normalmente toman medias proactivas como el bloqueo de las direcciones de protocolos de Internet hostiles.

En estas situaciones tradicionales, tratamos las redes como un elemento de apoyo. Es decir, nuestras redes necesitan funcionar sin interrupción para que puedan operar nuestras capacidades bélicas simétricas—lo que es análogo a decir que los camiones de reabastecimiento de combustible necesitan funcionar para que los F-16 puedan despegar. Es difícil contemplar la lucha en redes de EE.UU., pero las operaciones de NetD deben aprovecharse del acceso a las NetOps enemigas y responder disminuyendo la credibilidad de la información robada, aumentando el costo de un ataque a las redes de la Fuerza Aérea y del DOD, o permitiendo que Estados Unidos influya en las percepciones del adversario antes y durante todas las fases del conflicto.

Proponemos lo siguiente como forma de resaltar la utilidad de este nuevo concepto, que verdaderamente considera que la NetD es una forma de guerra asimétrica. Actualmente, cada OPLAN tiene un apéndice que trata los requisitos de la NetD. No obstante, además de proporcionar una protección preventiva de la red, los OPLAN futuros deben identificar los sistemas críticos para realizar operaciones de combate tradicionales (por ejemplo, redes logísticas, nódulos de comando y control, etc). Además, debemos identificar con precisión los adversarios que representa una gran amenaza de modo que podamos planificar y coordinar las operaciones de ciberenfrentamiento, y debemos planificar y ejecutar las operaciones de asignación de objetivos en sistemas críticos para la misión identificados por los COCOM. No obstante, esta vez si descubrimos al adversario, debemos comenzar las operaciones de enfrentamiento para afectarle o influirle.

Hay dos puntos importantes en los que merece la pena hacer énfasis. Primero, el adversario descubierto durante las operaciones de asignación de objetivos podría ser completamente diferente del tratado por el OPLAN—una posibilidad que hace que el ciberespacio sea un dominio difícil de dominar. En segundo lugar, las operaciones de asignación de objetivos y enfrentamiento no tienen necesariamente que estar enlazados a un OPLAN específico de un COCOM. Podemos realizar operaciones de asignación de objetivos proactivos siempre que podamos delinearlos y sincronizarlos debidamente con otras operaciones. Debemos considerar llevar a cabo operaciones de enfrentamiento cada vez que descubrimos una intrusión de la red, ya sea mediante técnicas de detección tradicionales u operaciones de asignación de objetivos.

Conclusión

Según la Escuadra Aérea de Guerra de Redes 67, "En resumidas cuentas la Fuerza Aérea debe efectuar la transición de una operación centrada en la detección a un método de una cadena de aniquilación de redes activa que integra prevención, detección, respuesta y enfrentamiento con el adversario".[13] Esta visión no puede fructificar sin organizar y asignar tareas unidades operacionales de NetD para cambiar sus conceptos operacionales desde un método reactivo (monitorear, detectar y responder) a uno que, según lo describió recientemente el Teniente General William T. Lord, "busca amenazas y . . . las detecta y destruye de forma instantánea".[14] No podemos hacer esto si estamos aislados. Necesitamos una planificación y una coordinación con un fin determinado con inteligencia y agencias de nivel nacional. Además, la creación del Cibercomando de EE.UU. debe ayudar a asegurarse de que los servicios actúen según la autoridad y la dirección de un COCOM. Los conceptos de asignación de ciberobjetivos y ciberenfretamiento "operacionalizan" verdaderamente la NetD, ya que se concentran completamente en actuar sobre el adversario y afectarle. En el futuro, debemos prestar una atención comparable a la certidumbre de la misión (por ejemplo, continuar las operaciones a pesar de los ataques del enemigo), un área que impide la separación completa de la NetD y las NetOps. No obstante, no podemos tratar esto de forma adecuada sin planificar y sin una inteligencia muy buena. El DOD gasta 100 millones de dólares de EE.UU. cada seis meses para defender la red .mil.[15] En cierto momento, nos debemos preguntar si estamos logrando nuestros objetivos defensivos y disuadiendo a los adversarios. Hoy, no lo estamos haciendo, pero al operacionalizar la NetD y concentrarnos sobre cómo afectar al enemigo, podemos invertir esta tendencia de modo que la Fuerza Aérea pueda contraatacar. ❑

Base de la Fuerza Aérea Lackland, Texas

Notas

1. Air Force Program Action Directive (Directiva de acción del programa de la Fuerza Aérea) 07-08, *Phase One of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces (Fase uno de la implementación del Secretario de la Dirección de la Fuerza Aérea para organizar las fuerzas ciberespaciales de la Fuerza Aérea)*, 19 de diciembre de 2008, 8.

2. Air Force Instruction (Instrucción de la Fuerza Aéra) 33-115, tomo 1, *Network Operations (Operaciones de redes) (NETOPS)*, 24 de mayo de 2006, 3, http://www.af.mil/shared/media/epubs/AFI33-115V1.pdf (visitada el 13 de mayo de 2010); y Air Force Doctrine Document (Documento de la Doctrina de la Fuerza Aérea) 2-5, *Information Operations (Operaciones de información)*, 11 de enero de 2005, 20, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5.pdf (visitada el 13 de mayo de 2010).

3. Publicación conjunta 3-13, *Information Operations (Operaciones de información)*, 13 de febrero de 2006, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (visitada el 13 mayo de 2010).

4. Spyros Antonatos y otros, "Defending against Hitlist Worms Using Network Address Space Randomization" (Defensa contra los gusanos informáticos usando la aleatorización del espacio de direcciones de la red), *Computer Networks* 51, no. 12 (22 de agosto de 2007): 3471–3490; y Dorene Kewley y otros, "Dynamic Approaches to Thwart Adversary Intelligence Gathering" (Métodos dinámicos para desbaratar la recopilación de inteligencia del adversario), en *Proceedings of the DARPA [Defense Advanced Research Projects Agency] Information Survivability Conference and Exposition*, (*Actas de la conferencia y exposición de supervivencia de información de la Agencia de Proyectos de Investigación de Defensa Avanzados*), tomo 1 (2001), 176.

5. "Engaging the Adversary on Air Force Networks" (Enfrentamiento con el adversario en las redes de la Fuerza Aérea), Information Assurance Technology Analysis Center Report (Reporte del Centro de Análisis de Tecnología de Certidumbre de Información), TAT 04-25, DO 232, 5 de marzo de 2007, 1.

6. Presidente del estado mayor conjunto, una lista de distribución, memorándum, tema: National Military Strategy for Cyberspace Operations (Estrategia Militar Nacional para las Operaciones Ciberespaciales) (sin anexo), 13 de diciembre de 2006, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (visitada el 14 de mayo de 2010).

7. Sun Tzu, *The Art of War (El arte de la guerra)*, traducción de Samuel B. Griffith (New York: Oxford University Press, 1963), 87.

8. *Atribución* significa el nivel de confianza con el que podemos identificar al adversario.

9. John P. Stenbit, secretario auxiliar de defensa para el comando, control, comunicaciones e inteligencia, a los

secretarios de los departamentos militares y otros, memorándum, tema: Guía para las acciones de respuesta de defensa de redes de computadoras, 26 de febrero de 2003, https://powhatan.iiie.disa.mil/cnd/cnd-ra-matrixand-memo.pdf (visitada el 14 de mayo de 2010).

10. Carl von Clausewitz, *On War (Sobre la guerra)*, editado y traducido por Michael Howard y Peter Paret (Princeton, NJ: Princeton University Press, 1976), 84.

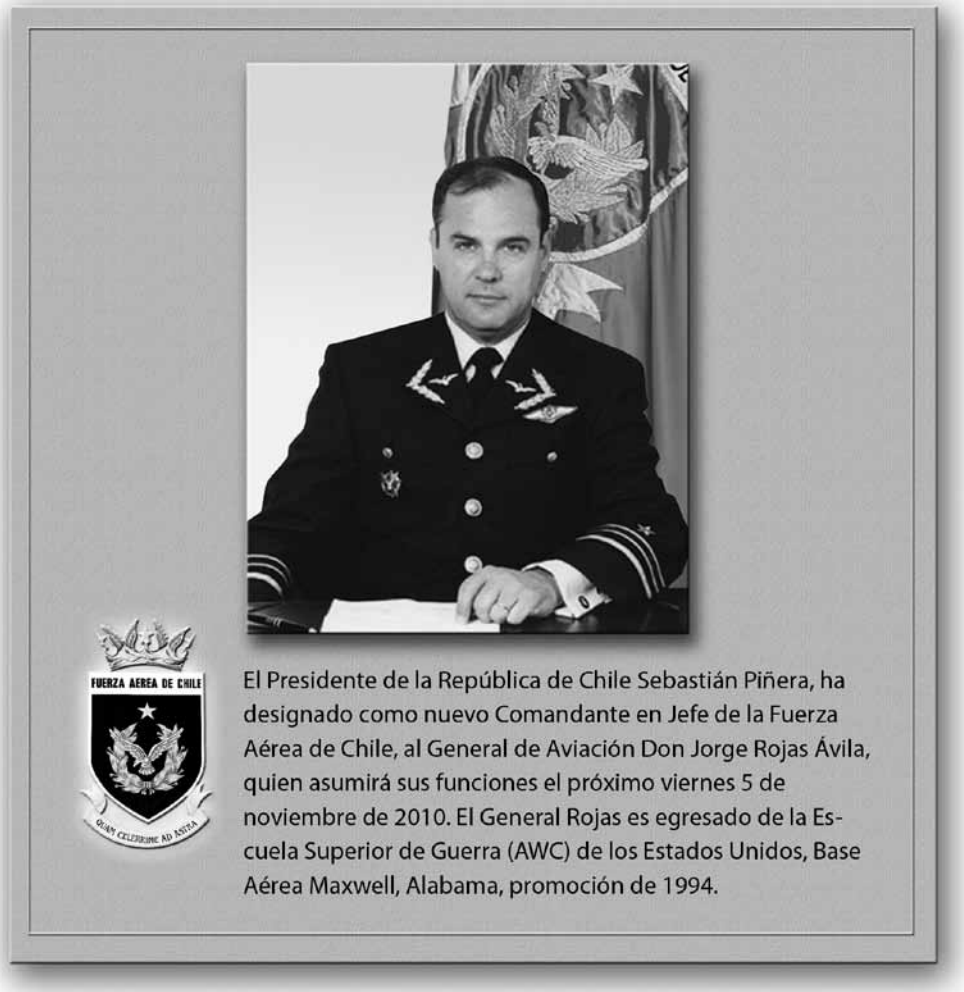
11. Manual de campaña 3-01.7, *Air Defense Artillery Brigade Operations (Operaciones de la brigada de artillería de defensa aérea)*, 31 de octubre de 2000, 6-36, http://www.theblackvault.com/documents/fm3_01x7.pdf (visitada el 14 de mayo de 2010).

12. Casa Blanca, *The National Strategy to Secure Cyberspace (La estrategia nacional para asegurar el ciberespacio)* (Washington, DC: La Casa Blanca, febrero de 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (visitada el 14 de mayo de 2010) .

13. Grupo de Operaciones de redes 26, "NetD Concept of Employment" (Concepto de empleo de la NetD), borrador final, 14 de diciembre de 2007, 2.

14. Chuck Paone, "General Calls for New Thinking on Cyberspace" (Llamadas generales para nuevas ideas en el ciberespacio), 12 de mayo de 2009, http://www.af.mil/news/story.asp?id=123148876 (visitada el 8 de abril de 2010).

15. William Jackson y Doug Beizer, "New DOD Cyber Command Will Focus on the Dot-Mil Domain" (El nuevo cibercomando del DOD se concentrará en el dominio. mil), *Government Computer News*, 15 de junio de 2009, http://gcn.com/Articles/2009/06/15/Web-DOD-cyber-command.aspx?p=1 (visitada el 8 de abril de 2010).



Declaración de responsabilidad: Las ideas y opiniones expresadas en este artículo reflejan la opinión exclusiva del autor elaboradas y basadas en el ambiente académico de libertad de expresión de la Universidad del Aire. Por ningún motivo reflejan la posición oficial del Gobierno de los Estados Unidos de América o sus dependencias, el Departamento de Defensa, la Fuerza Aérea de los Estados Unidos o la Universidad del Aire. El contenido de este artículo ha sido revisado en cuanto a su seguridad y directriz y ha sido aprobado para la difusión pública según lo estipulado en la directiva AFI 35-101 de la Fuerza Aérea.