El Auge de IPv6

Beneficios y costos de transformar el ciberespacio militar

Dr. Panayotis A. Yannakogeorgos, PhD

Mantener conciencia del avance de la tecnología y cosechar las oportunidades que ésta crea está en nuestra sangre como aerotécnicos innovadores. . . . Buscar la próxima tecnología "innovadora" es fundamental para mantener la ventaja asimétrica que nuestra Fuerza Aérea siempre ha proporcionado a la nación.

—Secretaria de la Fuerza Aérea, Deborah Lee James

Al prepararse la Fuerza Aérea de los Estados Unidos para una era de agilidad estratégica, nos entusiasman las tecnologías emergentes que ocupan los titulares, como el avión hipersónico, la nanotecnología y los sistemas autónomos y a control remoto que con el tiempo se convertirán en los facilitadores de misión fundamental.[1] Muy a menudo se pasan por alto los invisibles protocolos de conexión en red: protocolo de control de la transmisión (TCP) /protocolo Internet (IP) que revolucionaron a los militares y al mundo cambiando la forma en que los humanos intercambian y utilizan la información. Este protocolo de conexión en red mejora y habilita las cinco misiones fundamentales de la Fuerza Aérea: superioridad aérea y espacial, inteligencia, vigilancia y reconocimiento (ISR), movilidad global rápida, ataque global; y comando y control.

La Secretaria de la Fuerza Aérea, Deborah Lee James, señala en el reciente documento de estrategia *America's Air Force: A Call to the Future* (Fuerza Aérea de los Estados Unidos: Una llamada al futuro) que "esta estrategia reta a nuestra Fuerza Aérea a que siga adelante con una ruta de

agilidad estratégica —rompiendo paradigmas y aprovechando la tecnología tal como lo hicimos en nuestros comienzos".[2] Actualmente, el Departamento de Defensa (DOD), la Fuerza Aérea, y la nación están enfocados en las tecnologías que son importantes para el desarrollo futuro. Sin embargo, sin que lo sepa mucha gente, la estructura de Internet está cambiando por primera vez en su historia con el agotamiento del protocolo IP versión 4 (IPv4) y la adopción de IPv6. El DOD —así como la Fuerza Aérea en particular— tiene una tremenda oportunidad y responsabilidad para guiar a la nación en la transición a IPv6 para mejorar y habilitar las funciones y misiones fundamentales, asegurando la educación y capacitación de nuestros ciberoperadores para que mantengan el ritmo del cambio tecnológico.

Un informe reciente del inspector general del DOD encontró varios errores del oficial jefe de información (CIO) del departamento, Cibercomando Estadounidense, y la Agencia de Sistemas de Información de Defensa en cuando a dar prioridad a IPv6. La falta de coordinación y la negligencia del CIO para mantener un plan de acción, junto con hitos para la transición a IPv6, han costado al DOD tiempo y aumentará los costos.[3] En el transcurso de un estudio de desarrollo de ciberfuerza de trabajo de 18 meses de duración, el Instituto de Investigación de la Fuerza Aérea descubrió varias tendencias y percepciones preocupantes que contribuyeron a un entorno en el que IPv6 no tenía la alta prioridad de seguridad nacional que debería tener. Este artículo describe por qué debería tener una prioridad más alta y por qué los operadores y líderes principales por igual deberían preocuparse por el ritmo lento de la migración a IPv6 dentro del DOD.

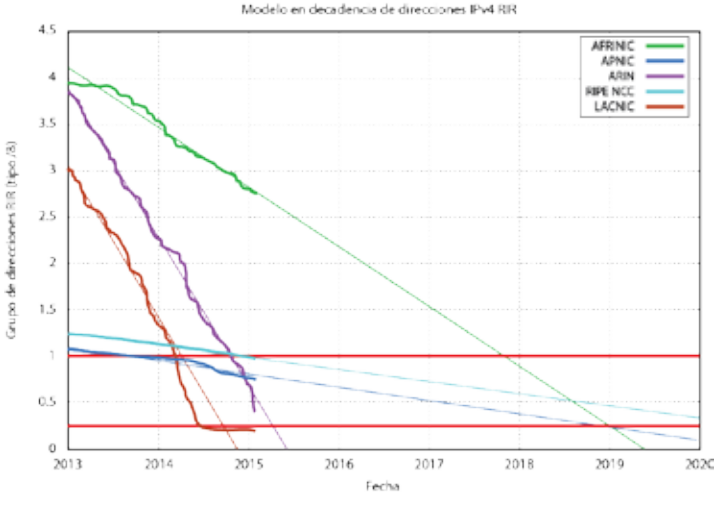

Figura 1. Proyección de consumo de los grupos de direcciones de registro Internet regional. (Del "Informe de direcciones IPv4", consultado el 29 de enero de 2015, http://www.potaroo.net/tools/ipv4/. Este informe fue generado el 29 de enero de 2015, a las 08:07 UTC. Reimpresión con permiso.)

AFRINIC - Centro de Información de Redes de África
APNIC - Centro de Información de Redes de Asia-Pacífico
ARIN - Registro Estadounidense de Números Internet
RIPE NCC - Centro de Coordinación de Redes del Réseaux IP Européens
LACNIC - Centro de Información de Redes de América Latina y el Caribe

El departamento investigó y desarrolló la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET), que eventualmente se convirtió en la Internet, cuando realizó la transición de ARPANET del protocolo de control de redes (NCP) al protocolo TCP/IP en 1981. El

DOD lideró al mundo en el desarrollo e implementación de protocolos y normas fundamentales de entrega de aplicaciones y servicios a los usuarios. Hoy, el núcleo de Internet, la manifestación más potente del ciberespacio, está a punto de cambiar por primera vez en la historia, y no estamos a la vanguardia. El protocolo de comunicaciones TCP/IP, un recurso Internet escaso y crítico, está realizando la transición de IPv4 a IPv6. Este último introducirá funciones en el entorno de conexiones en red, como la calidad del servicio y la multidifusión que mejorarán el intercambio y uso de la información. La voz sobre IP y la televisión sobre IP son solo dos de las aplicaciones que recibirán los beneficios de IPv6 y que revolucionarán cómo se comunica el mundo, tal como lo hicieron los satélites.[4] La necesidad de la transición de IPv4 a IPv6 no es hipotética ya que el suministro global de direcciones IP en IPv4 se está agotando rápidamente (figura 1).[5]

En el ámbito internacional, los pedidos para realizar la transición a IPv6 datan de 1996 y se intensificaron con la "Declaración de Montevideo" de 2013 de la Corporación de Internet para la Asignación de Nombres y Números (ICANN) que solicitaba que la "transición a IPv6 sea una alta prioridad a nivel global. En particular, los proveedores de contenido Internet deben proporcionar contenido utilizando los servicios IPv4 y IPv6, a fin mantener la accesibilidad de Internet global".[6] La transición del DOD y la Fuerza Aérea requerirá algo más que el simple accionar de un interruptor. Exigirá recursos importantes y el compromiso para la educación y capacitación de nuestra ciberfuerza de trabajo a fin de preservar las misiones en este dominio cambiante del que depende fuertemente el DOD.

¿Qué es una dirección IP y por qué la necesitamos?

Las máquinas se identifican entre sí en Internet y en la mayoría de las redes por medio de direcciones IP y de control de acceso a medios (MAC). Aunque invisibles, las direcciones IP son limitadas en número, lo que las convierte en un recurso Internet escaso y crítico. Todo equipo y software conectado en red debe tener un IP y dirección válidos para que funcionen en una red, sea en Internet abierta o en una red de control de sensores cerrada. En particular, identifican las máquinas, los paquetes de datos de guía y la información a través de redes de computadoras — incluyendo Internet. El uso de paquetes de datos, las unidades básicas del tráfico de red, es el método normal de dividir la información en unidades más pequeñas al enviarla por una red. Un componente vital de las redes, el encabezado IP, contiene información pertinente a las direcciones de origen y destino. Las máquinas necesitan estas cadenas de números para conectarse con otras computadoras en Internet o en otras redes.[7] La máquina receptora vuelve a crear los paquetes de datos en base a la información que contiene el encabezado de cada paquete de datos, que le indica a la computadora receptora cómo recrear la información a partir de los paquetes de datos. Sin protocolos de comunicación normalizados, como TCP/IP, no se podría garantizar que la máquina receptora pueda leer los paquetes de datos.[8]

Al cruzar la brecha digital más gente, organizaciones y máquinas, se van agotando las direcciones IP en la medida que los proveedores de servicios las asignan. Los procesos para asignar direcciones IP escasas y permitir que Internet sirva como una plataforma global son complejos. ICANN asigna el espacio de direcciones IPv4 a varios registros mediante la Autoridad de Asignación de Números de Internet (IANA) de acuerdo con la Administración Nacional de Telecomunicaciones e Información del Departamento de Comercio de los Estados Unidos, que actualmente controla la función procedimental de administrar cambios en el archivo de zona raíz del Sistema de Nombres de Dominio (DNS).[9] La IANA asigna el espacio de direcciones en bloques de prefijo tipo /8 (16,777,216 direcciones IP) para IPv4 a los registros regionales solicitantes según sea necesario.[10] El registro Internet regional (RIR) revende luego bloques tipo/16 más pequeños (64,000 direcciones IP) a los proveedores de servicio Internet (ISP) y a otras organizaciones. A continuación, los ISP revenden bloques más pequeños de espacio de direcciones IP a

los usuarios finales para que accedan a Internet (figura 2). La asignación de direcciones IPv6 es similar; sin embargo, está estructurada de manera que todas las redes IPv6 tengan espacio para 18.446.744.073.709.551.616 direcciones IPv6. En términos sencillos, cada red tendrá más espacio que el grupo completo de IPv4.[11]

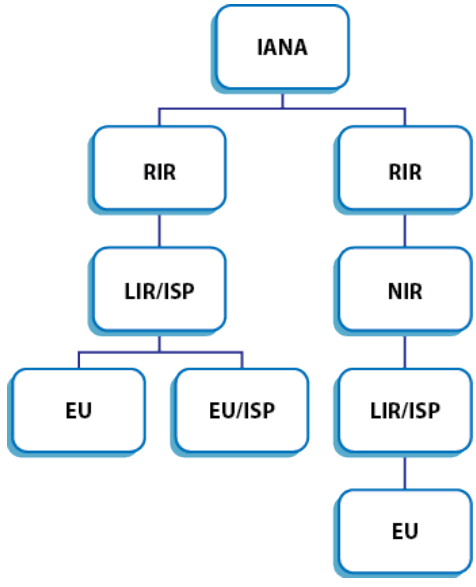

Figura 2. Jerarquía de asignación de direcciones
IANA: autoridad de asignación de números Internet
RIR: registro Internet regional
RIR: registro Internet local
ISP: proveedor de servicio Internet
NIR: registro Internet nacional
EU: usuario final

A diferencia de la concepción popular de una Internet sin límites, el espacio de direcciones subyacente es finito. De hecho, ya se ha agotado el espacio de direcciones de IPv4 para asignación por IANA y los registros de Internet regionales de Europa, Asia y América Latina. Anticipando esta eventualidad, los ingenieros desarrollaron IPv6 en la década de 1990. Entre otras mejoras, aumentó el número total de potenciales direcciones IP de 4.294.967.296 en IPv4 a 2128 en IPv6.[12] Aunque el protocolo IPv6 se ha podido implementar desde 1996, actualmente el mundo enfrenta una escasez de espacios de direcciones IPv4, en los que Internet se apoya actualmente. Este déficit solo podrá empeorar a medida que se intensifique el establecimiento de una "Internet de objetos". Al comunicarse las máquinas con otras máquinas, cada una de ellas necesitará su propia dirección IP. ICANN señaló en 2011 que la "futura expansión de Internet ahora depende de la implementación global exitosa de la siguiente generación del protocolo Internet, llamado IPv6".[13] Aunque los CIO dentro del DOD y el gobierno estadounidense admiten que el mundo está haciendo la transición de IPv4 a IPv6 como el protocolo de comunicaciones dominante para Internet global, no es evidente que la transición rápida sea una prioridad.

La ruta de la migración de la Fuerza Aérea

Dentro del servicio, el Centro de Integración de Redes de la Fuerza Aérea (AFNIC) viene trabajando desde 2002 en la transición de la Fuerza Aérea del formato de direcciones actual IPv4 al IPv6. La última fecha límite para la transición fue el mandato no obligante de 2014.[14] Sin embargo, la migración de la Fuerza Aérea tardará mucho más, teniendo en cuenta que el servicio no ha comenzado la migración de las capacidades básicas del servicio de redes, salvo en bases seleccionadas. Incluso los que han comenzado han dado marcha atrás en sus esfuerzos.[15] Aparte de unos cuantos laboratorios y la Red de Investigación e Ingeniería de Defensa, apenas media docena de máquinas en la Red del Direccionador de Protocolo Internet No Seguro (NIPR) de la Fuerza Aérea usan IPv6 legítimamente.[16] Aún así, se ha indicado que el plan involucra el uso de IPv4 y IPv6 en paralelo por los próximos 10 a 15 años. Este enfoque complica más el éxito operativo ya que esta estructura doble impone una carga de energía adicional en los procesadores para ejecutar ambos protocolos, negando potencialmente algunos de los beneficios de la transición completa. Además, introduce debilidades en el sistema.

¿Cuáles son los beneficios militares de la transición?

En su preámbulo en *America's Air Force: A Call to the Future* (Fuerza Aérea de los Estados Unidos: Una llamada al futuro), el General Mark A. Welsh III, Jefe de Estado Mayor de la Fuerza Aérea, enfatiza que "la capacidad de la Fuerza Aérea para adaptarse y responder más rápido que nuestros adversarios potenciales es el desafío más grande que enfrentamos en los próximos 30 años".[17] Desde luego, se puede escribir un artículo completo sobre el hecho de que China lidera al mundo en la implementación operativa de redes puramente IPv6 mediante su programa Internet de Próxima Generación de China.[18] Los efectos para la seguridad nacional estadounidense podrían ser considerables.[19] La capacidad de los actores extranjeros para dominar el campo de gobierno de Internet presenta un tremendo problema para nuestro actual entorno de seguridad. Sin embargo, la discusión de tales amenazas está fuera del alcance de este artículo. Esta sección se ocupa menos de la amenaza que de la utilidad de implementar redes nativas de IPv6 y la potencial vulnerabilidad de no hacerlo sin una estrategia para educar a nuestra ciberfuerza de trabajo en este nuevo entorno operativo.

Tanto para el DOD como para la Fuerza Aérea, IPv6 es una tecnología crucial que habilita teorías de guerra centradas en redes en apoyo de las cinco misiones fundamentales del servicio. Además del número básico de direcciones IP disponibles, IPv6 permite capacidades de conexión en red más avanzadas que IPv4. Las máquinas/sensores, dispositivos, aplicaciones, y servicios conectados en red se beneficiarán de la mejor funcionalidad de IPv6. Ciertamente, el resultado del estudio *Cyber Vision 2025* (Visión del ciberespacio 2025) del científico jefe de la Fuerza Aérea sugiere varias tecnologías que se podrían beneficiar enormemente del mayor espacio de direcciones que ofrece IPv6. La adopción del uso generalizado del protocolo sería especialmente ventajoso en las áreas de garantía y empoderamiento de la misión, así como en la mejora de la agilidad y resistencia de los sistemas que dependen de las capacidades del ciberespacio. Se podría aprovechar las ventajas de IPv6 para reducir el riesgo cibernético de las misiones de la Fuerza Aérea habilitando el salto de IP; arquitecturas mutantes; comunicaciones ágiles y tácticas; redes sensibles heterogéneas y operativas; y otras áreas transversales de la misión. *Cyber Vision 2025* reconoce estas ventajas de IPv6.[20] Sin embargo, las estrategias del CIO actual exigen que la transición a IPv6 total ocurra utilizando IPv4/IPv6 en paralelo y por fases.[21] El apilado doble o la ejecución de IPv4/IPv6 en paralelo es una mala idea. Primero, introduce vulnerabilidades de seguridad bien documentadas.[22] ¿Esperamos que nuestros adversarios potenciales no entiendan este hecho y no aprovechen las ventajas de IPv6, desafiando así nuestros esfuerzos en el ciberdo-

minio? Segundo, aumenta los costos de personal, ya que la fuerza de trabajo debe entender ambos sistemas.

El espacio de direcciones IP es importante para lograr los elementos de todas las misiones fundamentales de la Fuerza Aérea. Constantemente se hacen asignaciones, y los programas grandes exigen asignaciones grandes. Un ejemplo que ilustra este punto dentro del conjunto de misiones de movilidad global involucra al nuevo avión cisterna KC-46 actualmente en una línea de ensamblaje que debe producir 179 aviones en los próximos 20 años. Todos ellos necesitan espacio de direcciones IP. Toda misión de la Fuerza Aérea debe tener grandes espacios de direcciones IP por plataforma para apoyar una plataforma de comunicaciones robusta y redundante que requiere múltiples conmutadores de red para garantizar un comando y control resistente y los objetivos de la misión.

Otro ejemplo que resalta las ventajas se refiere a la capacidad de ISR integrada flexible y global que se exige en el documento de estrategia de la Fuerza Aérea: "Los requisitos ampliados y la amenaza creciente a los costosos activos aéreos también demandarán cambiar de una arquitectura centrada en plataformas ISR dedicadas a una plataforma basada en una red de sensores diversa organizada en los dominios aéreo, espacial y ciberespacial, imponiendo una prima en la capacidad de extraer datos de cualquiera y todos los sistemas estadounidenses".[23] El espacio de direcciones ampliado haría posible un número muy grande de sensores conectados en red en un vasto espacio de direcciones IP que ofrecería a los sensores sus propias direcciones IP estáticas. Además, los dispositivos de comunicaciones con direcciones IP estáticas propias que utilizan únicamente IPv6 consumirían menos energía, permitiendo de así una mayor duración de la batería en los dispositivos móviles en los que se apoya el comando y control de muchas operaciones militares.[24]

¿Por qué no hemos hecho la conversión hasta ahora?

Los mitos persistentes continúan poniendo obstáculos a las discusiones sobre la transición a IPv6.[25] Éstos caen principalmente en cuatro categorías: (1) arquitectura inmadura, (2) vulnerabilidades de seguridad, (3) el mito de que el DOD tiene suficientes asignaciones de direcciones IPv4, y (4) la carga fiscal de la conversión durante una época de austeridad.

Arquitectura inmadura

Algunos sostienen que el área de v6 no ha madurado lo suficiente como para forzar un cambio que incluya tecnología, arquitectura y destrezas de personal de operaciones. Una visión dentro de la Fuerza Aérea sostiene que no hay razones convincentes para IPv6 en este momento, y que la comunidad de ciberoperaciones tiene trabajo de sobra por el momento. Sin embargo, este argumento se estrella en dos puntos. Primero, el CIO y la Oficina de Responsabilidad del Gobierno de los Estados Unidos, tal como se señaló anteriormente, alientan el apilado doble. Segundo, la estrategia de la Fuerza Aérea declara que "una de las responsabilidades más importantes de un servicio militar es preparar a la fuerza para los desafíos de mañana, no solo para las realidades de hoy".[26] Es también claro que aunque la mayor parte de los equipos de tecnología de información (TI) tiene capacidad de IPv6, la Fuerza Aérea no tiene planes importantes para hacer uso de esta capacidad en el futuro inmediato (dos a cinco años).[27] En el presente, el mayor desafío operacional es asegurar que se desactiven las nuevas capacidades de tunelización de v4 a v6, y viceversa, para que nuestros adversarios no las puedan aprovechar.[28]

Vulnerabilidades de seguridad

Un desafío futuro clave es que aunque se habiliten v4 y v6 durante un período de transición, según el Instituto Nacional de Normas y Tecnología (NIST) "es probable que prevenir el acceso no autorizado a las redes IPv6 sea más difícil en los primeros años de la implementación de IPv6".[29] De hecho, contrario a la sabiduría convencional, existen serias debilidades de seguridad que vas más allá de activar el equipo de conexión en red que la Fuerza Aérea ya ha adquirido. La NIST advierte que,

> Al aumentar la difusión del protocolo IPv6, las redes empresariales y conectadas a Internet necesitarán estar preparadas para amenazas y vulnerabilidades específicas que traerá el nuevo protocolo. Por ejemplo, el segmento de redes puramente IPv4 puede contener varios host de recién instalados que son compatibles con IPv4 y IPv6, y también hosts que de forma predeterminada están habilitados para IPv6. Esta circunstancia puede ocurrir simplemente como resultado de los ciclos de vida de los sistemas normales. Además, un atacante podría habilitar IPv6 en un host para eludir los controles de seguridad que IPv6 podría no conocer; estos host pueden ser utilizados posteriormente para crear canales encubiertos o de puerta trasera. Yendo más lejos, el tráfico de IPv6 podría ser encapsulado dentro de paquetes de IPv4 usando herramientas y servicios de fácil acceso, e intercambiado con hosts maliciosos a través de Internet.[30]

Las consecuencias pueden incluir la incapacidad de muchas herramientas de defensa y forenses basadas en host para controlar el enorme espacio de direcciones de las redes IPv6. La subred IPv6 más pequeña será 4 mil millones de veces más grande que el intervalo completo de IPv4; en consecuencia, los defensores tendrán dificultad para encontrar víctimas. Un dispositivo explorador de IPv6 podría tardar días o semanas en localizar todos los host en la red de la Fuerza Aérea, ni qué decir escanearlos por vulnerabilidades. Los sistemas de detección de intrusiones de IPv4 existentes no pueden verificar el contenido de un paquete tunelizado en IPv6 y viceversa. Así, se asociará un costo financiero con la adquisición de sistemas para defender las redes v4 y v6. Esto, además del costo de educar y capacitar a nuestros ciberoperadores, así como del establecimiento de herramientas de defensa de redes para detectar la amenaza potencial de exactamente lo opuesto a tunelizar IPv4 sobre IPv6. Por lo tanto, aunque la adopción del apilado doble generalizado es una meta admirable, hacerlo tendrá un efecto en cada uno de los protocolos de tunelización sobre producción, tasas de datos y latencia resultantes.

El mito que la asignación de direcciones IPv4 del Departamento de Defensa es suficiente

Otra percepción errónea que impregna la discusión es que el agotamiento de IPv4 no es un problema para el DOD ya que se ha reservado una gran asignación de direcciones IPv4 a nivel mundial para fines de seguridad nacional.[31] Históricamente, el DOD ha sido un almacén de experiencia técnica relacionada con Internet, dadas las raíces de Internet dentro de la Agencia de Proyectos de Investigación Avanzada de Defensa; su operación del dominio ".MIL", un dominio de nivel superior exclusivo para uso del DOD; y su manejo de los servidores de nombres DNS para apoyarla. A principios de la década de 1990, el DOD adquirió una cantidad importante de espacio IPv4 —12 bloques de espacio de bloques tipo /8. Como cada bloque tipo /8 contiene 16.777.214 direcciones IP, el DOD tiene más de 200 millones de direcciones disponibles en el espacio v4. La situación actual con IPv6 es análoga a la de IPv4 a comienzos de la década de 1990. El DOD ha comprado un bloque tipo /13 de espacio v6, el equivalente de 42.000.000.000.000.000.000.000.000.000.000.000.000 espacios de direcciones IP.[32]

La sabiduría convencional en gran parte de la Fuerza Aérea es que el DOD y la Fuerza Aérea no tienen razones para preocuparse del agotamiento de las direcciones IP. Efectivamente, solo

un pequeño porcentaje de la red de la Fuerza Aérea utiliza direcciones IP de esas 12 asignaciones. Gran parte de esa red es anterior a la asignación de esas redes tipo /8, y sesga las proyecciones del DOD si suponemos que esas 12 redes tipo /8 es todo lo que dispone para trabajar. Por lo tanto, un análisis preciso considerará las direcciones IPv4 reales que está utilizando la Fuerza Aérea, gran parte de las cuales fueron adquiridas directamente antes de que el DOD recibiera sus grandes asignaciones.[33] Los cálculos en la base de datos "WHOIS" del Centro de Integración de Redes del DOD, a disposición del público, revelan que el departamento tiene algo más de 317 redes tipo /16 en su lista actual de redes de reserva que han sido recuperadas para asignación futura.[34] También existe una mezcla de asignaciones más pequeñas. De las 317 redes tipo/16, actualmente se mantiene en reserva una red tipo /8 (29.0.0.0/8) no utilizada. Si el objeto de hacer esto es para apoyar a la totalidad del DOD, entonces no es un espacio de direcciones adecuado para las futuras aplicaciones.

Dentro de la Fuerza Aérea, los promedios anuales de la tasa de agotamiento de IPv4 no muestran claramente una tendencia de aumento o disminución de las tasas de consumo (figura 3). Los números anómalos en 2010 fueron causados por una limpieza de redes que reparó problemas de larga data y deben considerarse como algo atípico. Usando estos números en una ruta de agotamiento lineal, encontramos que la fecha de agotamiento proyectada de la totalidad del espacio de direcciones IP que posee le Fuerza Aérea es el 31 de diciembre de 2029, aunque es más probable que ocurra antes de esa fecha debido a las demanda creciente de espacio de direcciones IP al ponerse en servicio nuevos sistemas que demandan más de este recurso limitado. Por lo tanto, la idea que el DOD y la Fuerza Aérea no tienen que preocuparse por el agotamiento de IPv4 es un mito. El planeamiento para la conversión inevitable debe empezar lo antes posible ya que es probable que los aliados se queden sin espacio de direcciones IPv4 mucho antes de 2029.

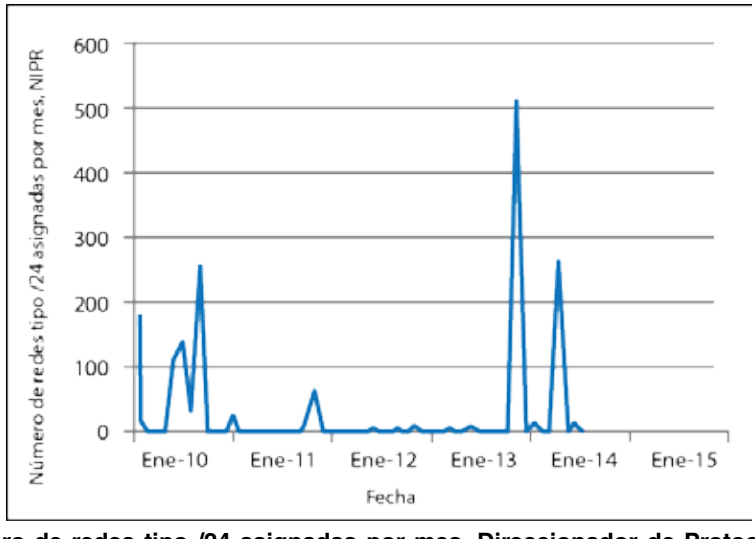

Figura 3. Número de redes tipo /24 asignadas por mes, Direccionador de Protocolo Internet No Seguro

El documento *Call to the Future* (Una llamada al futuro) de la Fuerza Aérea (Tercer Trimestre 2015), es claro en su creencia de que las guerras de la coalición serán cruciales para el éxito del

servicio durante los próximos 30 años: "De hecho, los escenarios más probables y más exigentes consideran que la Fuerza Aérea trabajará junto con, o liderando, aerotécnicos de la coalición".[35] Indudablemente, esta posibilidad ya es un reto.[36] Cuando las naciones socias y aliadas cambien sus redes nacionales y militares a IPv6, si lo hacen, la interoperabilidad entre nuestras redes y las redes aliadas/coalición no será posible sin técnicas de transición o conversión entre los dos protocolos. Esa situación aumentará la vulnerabilidad de las misiones operativas. Para aliviar esta debilidad, el NIST recomienda en sus *Pautas para la Implementación Segura de IPv6* bloquear todo el tráfico IPv6 en las redes puramente IPv4.[37]

La penetración de IPv6 está aumentando a nivel mundial, incluyendo Estados Unidos.[38] Sin embargo, el DOD no está manteniendo el ritmo debido a la percepción de que teniendo muchas direcciones IPv4 asignadas al dominio .MIL no se necesita la transición. Para mantener la interoperabilidad, el DOD deberá estar en IPv6 y ser capaz de trabajar con sistemas puramente IPv6 en el futuro. Es necesario disponer de tiempo para desplegar y capacitar operadores a fin de que empleen y defiendan con éxito un sistema nuevo. Por lo tanto, es necesario comenzar lo antes posible.

La carga fiscal de la conversión durante una época de austeridad

Finalmente, los que oponen a la conversión rápida a IPv6 también plantean el problema de la carga financiera asociada con la transición. Desde luego, se necesitarán fondos adicionales para cubrir el costo de nueva infraestructura y servicios de red. Por consiguiente, según los críticos, en un medio de presupuesto limitado con prioridades que compiten, el momento no es adecuado para realizar la transición. Este argumento es parcialmente cierto. Debido a que el DOD fue pionero de Internet, Estados Unidos posee una infraestructura antigua muy grande basada en IPv4. Por lo tanto, el costo de la transición será más alto que en las organizaciones que no dispongan de una infraestructura antigua. Las naciones y organizaciones con poca infraestructura podrán comenzar directamente con una infraestructura compatible con IPv6, utilizando métodos como apilado doble durante el período de transición y luego desactivando IPv4. Sin embargo, el AFNIC ha sido partidario de IPv6 desde 2002. El uso de las herramientas disponibles y el énfasis en las estrategias centradas en la compra de equipos compatibles con IPv6 fueron actualizados durante el ciclo de actualización técnica normal de 2003, cuando el DOD exigió que todo el equipo y software "desarrollado, procurado o adquirido sea compatible con IPv6 (además de mantener la interoperabilidad con los sistemas/capacidades de IPv4)".[39] La Ley de Autorización de Defensa Nacional también incluye un elemento de inspección de IPv6 que el CIO de la Fuerza Aérea puede utilizar como medida de efectividad de las boletas de calificaciones de cada programa: "El PM [gestor de programa] debe iniciar los esfuerzos para la transición de los sistemas y aplicaciones de IPv4 para soportar IPv6 y determinar el impacto en IPv6. El PM deberá realizar un análisis que determine los impactos en el costo y la programación necesarios para modificar el sistema. El PM deberá incluir requisitos de IPv6 en el presupuesto de adquisición de programas y actualización de tecnologías y en las solicitudes del memorándum de objetivos del programa".[40] Una mala puntuación en esta boleta de calificaciones podría retrasar los fondos de un programa.[41] Los reglamentos de adquisición federal también ordenan que se procure equipos IPv6 en cualquier compra posterior a diciembre de 2009, fecha en que apareció el requisito de IPv6.[42] Las figuras 4-6 muestran el estado de habilitación de IPv6 en la Fuerza Aérea y el DOD.

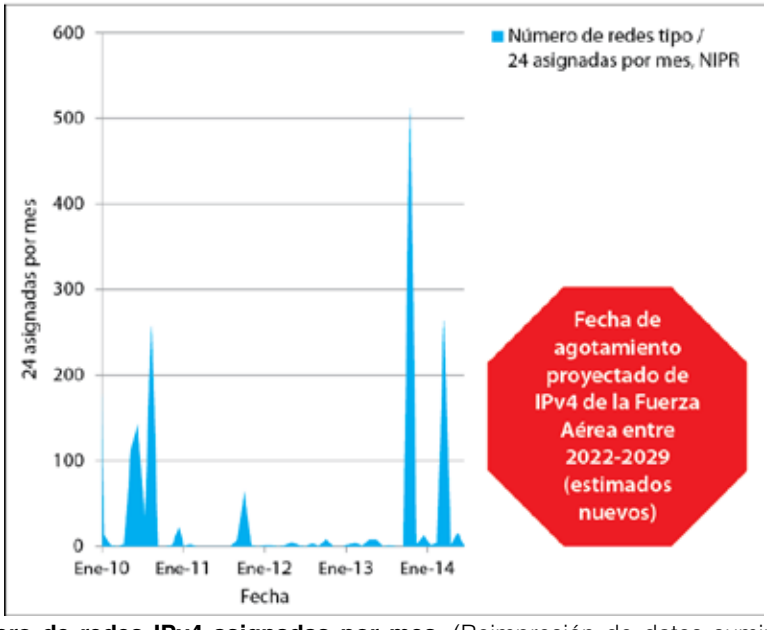

Figura 4. Número de redes IPv4 asignadas por mes. (Reimpresión de datos suministrados por la Oficina de Redes de Sistemas de la Fuerza Aérea.)
NIPR - Red de direccionadores de protocolo Internet no seguro

Figura 5. Dominios habilitados para IPv6 completos, Departamento de Defensa. (Reimpresión de "Estimating IPv6 & DNSSEC External Service Deployment Status, Department of Defense (Estimación del estado de implementación de servicios externos para IPv6 y DNSSEC, Departamento de Defensa)", Laboratorio de Tecnología de Información, División de Tecnologías Avanzadas de Redes, Instituto Nacional de Normas y Tecnología, consultado el 2 de febrero de 2015, http://fedv6-deployment.antd.nist.gov/cgi-bin/cfo?agency=defense.)

Figura 6. Servicios habilitados para IPv6, Departamento de Defensa. (De "Estimating IPv6 & DNSSEC External Service Deployment Status, Department of Defense (Estimación del estado de implementación de servicios externos para IPv6 y DNSSEC, Departamento de Defensa)", Laboratorio de Tecnología de Información, División de Tecnologías Avanzadas de Redes, Instituto Nacional de Normas y Tecnología, consultado el 2 de febrero de 2015, http://fedv6-deployment.antd.nist.gov/cgi-bin/cfo?agency=defense.)

Por lo tanto, de acuerdo con los reglamentos de adquisiciones, los equipos se han comprado durante los ciclos de actualización técnica. A medida que se compran nuevos dispositivos, artefactos e infraestructura adicional y se reemplaza el equipo antiguo, el equipo nuevo debe ser capaz de IPv6 —y eso no ha sido un problema. No obstante, el DOD se ha retrasado en las aplicaciones y sistemas que no son compatibles con IPv6. El AFNIC debe trabajar con el Sistema Empresarial de la Fuerza Aérea para desarrollar una ruta para implementar el cumplimiento de IPv6 en todos los servicios y aplicaciones digitales que aprovecharán los beneficios de IPv6 en las operaciones militares.

A pesar de los pocos costos de equipo (si los hay), no podemos argumentar que la transición a IPv6 no involucre gastos. Si la Fuerza Aérea y el DOD mantienen la ruta actual, es casi seguro que habrán más dificultades financieras debido a los requisitos de mano de obra; específicamente, la Fuerza Aérea y el DOD necesitarán dos grupos de administradores de redes —uno capacitado para IPv4 y otro para IPv6. De hecho, en una *Evaluación del impacto económico de IPv6, el NIST* estimó el costo de capacitación de una persona de gama alta como $2.906, siendo los costos totales mucho más altos (ver la tabla a continuación).[43] De hecho, el mismo informe indica que mientras más acelerada sea la transición a IPv6, mayor será el costo.

Tabla. Resumen de los costos de transición de IPv4 a IPv6

	Costos (Valor presente en millones de dólares de 2003)[a]
Proveedores de infraestructura	$1.384
Proveedores de aplicaciones	$593
Proveedores de servicio Internet	$136
Usuarios	$23.321
Total	$25.434

a Calculados con una tasa de descuento real de 7 por ciento

Fuente: Reimpresión de Michael P. Gallaher y Brent Rowe, *Planning Report 05-2, IPv6 Economic Impact Assessment* (Informe de planificación 05-2, Evaluación del impacto económico de IPv6) (Washington, DC: NIST, Departamento de Comercio de los Estados Unidos, Administración de Tecnologías, octubre de 2005), ES-4, http://www.nist.gov/director/planning/upload/report05-2.pdf.

Recomendaciones

Exigir una fecha firme de transición a IPv6 utilizando las políticas de adquisición del DOD y el entorno de información conjunto

Actualmente no hay en el entorno de la Fuerza Aérea el nivel de compromiso y la voluntad para asumir el riesgo y empezar la migración de los servicios. El DOD ha olvidado la historia de conversiones de protocolos. Cuando ARPANET se desplegó por primera vez, no se basaba en TCP/IP, era una implementación de NCP. Basándose en investigaciones adicionales entre 1973 y 1981, se desarrolló TCP/IP a fin de permitir mejoras en las redes de intercambio de paquetes que existían, permitiendo que surja la "conexión entre redes" como una arquitectura de redes —y así, "nació" Internet. De hecho, el *Plan de Transición de NCP/TCP* proclamó en noviembre de 1981: "el Departamento de Defensa ha adoptado recientemente el concepto de Internet y los protocolos IP y TCP, en particular, como las normas generales del DoD para todas sus redes de paquetes, y hará la transición a esta arquitectura en el transcurso de los próximos años. Todas las redes de paquetes del DoD usarán exclusivamente estos protocolos".[44] La transición a TCP/IP tuvo éxito solamente gracias a la exigencia firme. Específicamente, el *Plan de Transición de NCP/TCP* ordenaba un "cambio completo de NCP a IP/TCP para el 1 de enero de 1983." Es tarea de cada organización principal implementar IP/TCP para sus propios equipos host. Esta tarea de implementación debe empezar el 1 de enero de 1982".[45]

Los líderes de la Fuerza Aérea deben aplicar un mandato similar hoy. En el pasado se han intentado fechas de transición firmes con IPv6 —por ejemplo, en una orden de la Oficina de Administración y Presupuesto (OMB) en agosto de 2005, y el 28 de septiembre de 2010 otro memorándum de la OMB ordenó la transición federal a IPv6.[46] La Fuerza Aérea admitió la necesidad de realizar la transición pero no estableció una orden enfática para el esfuerzo. El requisito más contundente fue el memorándum de la OMB de agosto de 2005 que incluyó fechas que todos tratan de ignorar. Es decir, sin un énfasis del A6/CIO de la Fuerza Aérea que ordene una fecha firme para la migración especificando multas por incumplimiento, es poco probable que se implemente la migración.

Ha llegado el momento de implementar esta migración en todo el DOD. De acuerdo con el desarrollo e implementación del entorno de información conjunto (EIC), "a fin de facilitar la implementación del EIC mediante adquisición en todo el Departamento, los nuevos programas de TI deberán cumplir con el EIC. Los programas de TI existentes deberán cumplir los requisitos del EIC a medida que avancen por su ciclo de vida, y se tomarán decisiones para que garantizar el mejor complimiento con EIC".[47] De hecho, el DOD ha ordenado que se complete esta migración a más tardar al final del año fiscal 2018.[48] Los críticos pueden argumentar que la dependencia en IPv4 es hoy más fuerte y más integrada en las operaciones militares cotidianas. Aunque esa afirmación es cierta, el desarrollo del EIC ofrece a la oficina del CIO del DOD una oportunidad para hacer una pausa en este esfuerzo e incluir un lenguaje que alinee la preparación de la red del EIC con un plan de implementación obligatorio de IPv6 que haga la transición del EIC a IPv6 para el fin del año fiscal 2018. El hacerlo contribuirá a asegurar que el DOD tenga hosts IPv6 habilitados y servicios desplegados, permitiendo así el cambio de paradigma al entorno IPv6. Por lo tanto, suponiendo que el EIC se implementa en algún momento antes de 2030, el DOD y la Fuerza Aérea no deberán enfrentar problemas de agotamiento del espacio de direcciones de IPv4 antes de la migración a EIC y IPv6.

Educar y capacitar a nuestros ciberoperadores en IPv6

Actualmente las escuelas cibernéticas de la Fuerza Aérea ofrecen algo de información general sobre IPv6 en el plan de estudios —en el mejor de los casos, dos horas de instrucción. Esta can-

tidad no es suficiente. Es necesario exigir una capacitación detallada, específica en IPv6, pero algunos creen que no hace falta ya que no representa la realidad operativa actual.[49] Más bien, la preferencia es reservar ese tipo de capacitación para las futuras unidades de adiestramiento en el campo cibernético que actualizarán a los operadores en los últimos avances de nuestras capacidades reales mientras realizan sus asignaciones. Este razonamiento es peligroso ya que es importante la experiencia en ciberoperaciones. Tal como se indicó antes, nuestros competidores chinos, entre otros, están adquiriendo experiencia en la operación de redes IPv6 mientras que la Fuerza Aérea está ignorando el problema. Para resolver este dilema, el servicio debería comenzar la educación y capacitación de los ciberguerreros del futuro en IPv6 tan pronto como lo permitan los procesos de diseño de currículo del Comando de Educación y Capacitación Aérea (AETC) y del Comando Espacial de la Fuerza Aérea (AFSPC).

Los elementos importantes que se deben incluir en una carta de asignación de capacitación de los administradores de campo profesional y la Vigésimo Cuarta Fuerza Aérea a las unidades de educación y capacitación de AETC y AFSPC incluyen, sin limitarse a ellas, actualizaciones del currículo que cubran los siguientes temas específicos de IPv6 que son susceptibles a vulnerabilidades al emplearse:

- descubrimiento/enumeración de receptor de multidifusión;
- descubrimiento/enumeración de direccionador;
- consulta de nodos;
- protocolo de datagramas de usuario (UDP)/cálculo de sumas de comprobación TCP;
- mecanismos de transición 6to4, 6in4, 6over46rd, 4rd, Teredo, protocolo de direccionamiento de tunelización automática dentro del sitio (ISATAP);
- configuración automática de direcciones apátridas (SLAAC);
- protocolo de descubrimiento de vecino seguro (SeND);
- protocolo de descubrimiento de vecino;
- detección de dirección duplicada;
- direccionador, protocolo de control de host dinámico (DHCP), y descubrimiento de DNS;
- redireccionamiento;
- nuevas funciones en DHCPv6; y
- movilidad de host y de red para los sistemas tácticos, satelitales y de aeronaves.

Debido a que las operaciones en el ciberespacio requieren experiencia práctica, podría ser necesario considerar financiamiento adicional y la creación de un intervalo de IPv6 en las bases Keesler y Hurlburt de la Fuerza Aérea, donde la Escuela de Cibercapacitación de Licenciatura y el Escuadrón de Operaciones de Información No. 39 realizan la capacitación. Los críticos podrían argumentar que el currículo no incluye suficientes horas para IPv4 y IPv6. Sin embargo, dada la interrelación entre IPv4 y IPv6, al enseñarse v6 en efecto se estaría también enseñando v4. Además, la Fuerza Aérea debe asegurar que los aerotécnicos que ya están en el campo profesional obtengan una mayor exposición a v6. Una solución de corto plazo sería alentar la inscripción en el Entorno de Capacitación Virtual Federal al desarrollar la AECT y el AFSPC más soluciones de capacitación de largo plazo.

Conclusiones

La transición a IPv6 no es un escollo demasiado difícil de superar. No es una tecnología subdesarrollada ni sin ensayar. Más bien, la transición es un problema de política desconectada de las realidades tecnológicas. La migración a IPv6 debe ser una preocupación principal de nues-

tros líderes superiores, y parece que solo un compromiso y mandato claro estimulará la transición necesaria. Cuando esto ocurra, se debe poner en efecto una estrategia que garantice que esta transición no sea una solución de ejecución precipitada sino una solución que tenga metas y mapas de ruta claros para la implementación segura de IPv6 a través de la Fuerza Aérea. En cuanto al DOD, el EIC es un lugar excelente para comenzar el despliegue total de IPv6 y evitar los costos adicionales de una transición tardía, incluyendo el posible fracaso de la misión. Nuestros ciberoperadores deben comenzar la capacitación desde ahora en el entorno operativo en el que ciertamente estarán inmersos en la próxima década. La protección de la red y el desarrollo de la próxima generación de tácticas, técnicas y procedimientos para las operaciones en el ciberespacio hará posible la ejecución rápida y segura de las misiones fundamentales de la Fuerza Aérea. El aprovechamiento de IPv6 es crucial si el servicio debe seguir siendo la fuerza mejor equipada, capacitada y más mortífera del planeta. ❑

Notas

1. La investigación fue apoyada parcialmente por la Beca de la Oficina de Investigación Naval N000141310878 y la Iniciativa de Investigación Minerva del Departamento de Defensa.

2. Cuartel General de la Fuerza Aérea de los Estados Unidos, *America's Air Force: A Call to the Future (Fuerza Aérea de los Estados Unidos: Una llamada al futuro)* (Washington, DC: Cuartel General de la Fuerza Aérea de los Estados Unidos, julio de 2014), 4, http://airman.dodlive.mil/files/2014/07/AF_30_Year_Strategy_2.pdf.

3. Michael Peck, "DoD Fumbled IPv6 Transition, IG Says (El DoD actuó torpemente en la transición a IPv6, dice el Inspector General)", C4ISR&Networks, 5 de diciembre de 2014, http://www.c4isrnet.com/article/20141205/C4ISRNET/312050009/.

4. Las aplicaciones del protocolo de voz sobre Internet (VOIP), por ejemplo, que funcionan en IPv4 a veces pierden paquetes de datos, haciendo que las comunicaciones sean confusas. Con la función de calidad de servicio en IPv6, este problema desaparecería porque cada paquete de datos de VOIP se marca y entrega en una manera que impide la confusión de datos.

5. Para ver informes diarios sobre el estado de la tasa de agotamiento de IPv4, visite "IPv4 Address Report (Informe de direcciones IPv4)", consultado el 3 de febrero de 2015, http://www.potaroo.net/tools/ipv4/.

6. "Montevideo Statement on the Future of Internet Cooperation (Declaración de Montevideo sobre el Futuro de la Cooperación en Internet)", Corporación de Internet para la Asignación de Nombres y Números, 7 de octubre de 2013, https://www.icann.org/news/announcement-2013-10-07-en.

7. Elihu Zimet y Edward Skoudis, "A Graphical Introduction to the Structural Elements of Cyberspace (Una introducción gráfica a los elementos estructurales del ciberespacio)", en *Cyberpower and National Security*, editores Franklin D. Kramer, Stuart H. Starr, y Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 91–112. Véase también Robert E. Molyneux, *The Internet under the Hood: An Introduction to Network Technologies for Information Professionals (La Internet bajo el capó: Una introducción a las tecnologías de redes para profesionales de la información)* (Westport, CT: Libraries Unlimited, 2003), 85–86.

8. Molyneux, *Internet under the Hood (Internet bajo el capó)*, 27. Para los que no son expertos, una forma fácil de pensar en la importancia de la normalización en las telecomunicaciones internacionales es cómo nos conectamos a las redes de distribución eléctrica mientras viajamos. Debido a que los adaptadores eléctricos no están normalizados, los viajeros deben obtener un adaptador para enchufar su aparato en los enchufes de otros países si esa región no es compatible con la región de origen del viajero. Con la electricidad viene el peligro añadido de voltajes y ciclos no normalizados. Por lo tanto, los viajeros deben también averiguar si su aparato se quemará o no al conectarlo a una red de 220 voltios cuando el aparato puede recibir solo 110 voltios de energía.

9. La función de IANA, actualmente parte de un acuerdo de cooperación con el Departamento de Comercio de los Estados Unidos, está en las fases iniciales de una transición a ICANN, estando pendiente la aprobación de una propuesta de ICANN a NTIA sobre la transición. "NTIA Announces Intent to Transition Key Internet Domain Name Functions (NTIA anuncia la intención de realizar la transición de funciones clave de nombres de dominios Internet)", Administración Nacional de Telecomunicaciones e Información, 14 de marzo de 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

10. "Making Internet Number Resource Allocations to Regional Internet Registries (Asignaciones de recursos de números Internet a los registros de Internet regionales)", IANA, consultado el 3 de febrero de 2015, http://www.iana.org/help/inr-request-procedure. La IANA distribuye el espacio IPv4 en bloques de tipo /8.

11. "Understanding IP Addressing (Explicación del direccionamiento IP)", Centro de coordinación de redes RIPE, 22 de abril de 2014, http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing.

12. "Internet Protocol, Version 6 (IPv6) Specification (Especificación del protocolo Internet, versión 6 (IPv6))", Grupo de Trabajo de Ingeniería Internet, diciembre de 1998, http://tools.ietf.org/html/rfc2460.

13. "Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied: The Future Rests with IPv6 (El grupo disponible de direcciones Internet IPv4 sin asignar se ha agotado por completo: El futuro depende de IPv6)", ICANN, 3 de febrero de 2011, https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf.

14. Katherine Kebisek, "AFNIC Prepares Air Force for IPv6 Transition (AFNIC prepara a la Fuerza Aérea para la transición a IPv6)", Comando Espacial de la Fuerza Aérea, 4 de abril de 2011, http://www.afspc.af.mil/news1/story.asp?id=123249968.

15. Intercambio de correo electrónico entre el autor y personal del AFNIC, 21 de abril de 2015.

16. Agradezco al grupo Air Force Systems Networking (Redes de sistemas de la Fuerza Aérea) (AFSN) por esta observación.

17. Cuartel General de la Fuerza Aérea de los Estados Unidos, *America's Air Force*, 5.

18. Por ejemplo, el gobierno de China logró el hito histórico de organizar un evento global con una infraestructura IPv6 nativa durante los Juegos Olímpicos de Verano de 2008. Durante 1936 los nazis difundieron las Olimpiadas en directo para todo el mundo.

19. Panayotis A. Yannakogeorgos, "Internet Governance and National Security (Gobierno de Internet y seguridad nacional)", *Strategic Studies Quarterly* 6, no. 3 (Otoño de 2012): 102-25.

20. Mark T. Maybury, *Cyber Vision 2025 (Visión del ciberespacio 2025)* (Washington, DC: Científico Jefe de la Fuerza Aérea de los Estados Unidos, 13 de diciembre de 2012), 24, https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1355090FB5E044080020E329A9/Files/editorial/00Cyber%20Vision%202025%20FINAL%203-21-13.pdf.

21. Comisión de Estrategia y Planificación, Consejo de Oficiales Jefes de Información Federal, *Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government* (Guía de planificación/Mapa de ruta para la adopción de IPv6 dentro del gobierno estadounidense), versión 2.0 (Washington, DC: Comisión de Estrategia y Planificación, Consejo de Oficiales Jefes de Información Federal, julio de 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf.

22. Carlos E. Caicedo, James B. D. Joshi, y Summit R. Tuladhar, "IPv6 Security Challenges (Desafíos de seguridad de IPv6)", *IEEE Computer* 42, no. 2 (febrero de 2009): 36–42. Véase también Harith Dawood, "IPv6 Security Vulnerabilities (Vulnerabilidades de seguridad de IPv6)", *International Journal of Information Security Science* 1, no. 4 (2012): 100–105.

23. Cuartel General de la Fuerza Aérea de los Estados Unidos, *America's Air Force*, 15.

24. Stephen Lawson, "IPv6 Can Boost Mobile Performance, Battery Life, Proponents Say (IPv6 puede aumentar el rendimiento de los dispositivos móviles, la duración de la batería, dicen sus proponentes)", *Computer World*, 11 de enero de 2013, http://news.idg.no/cw/art.cfm?id=96C2FD24-B840-8D62-606480F34A52909D.

25. Los puntos saltantes en esta sección son una compilación de las observaciones realizadas en el transcurso de 15 meses de entrevistas en apoyo de un estudio sobre el desarrollo de la ciberfuerza de trabajo ordenado por el Jefe de Estado Mayor de la Fuerza Aérea (próxima publicación de Air University Press) así como de la investigación realizada durante el proyecto Minerva de la Oficina del Secretario de Defensa, METANORM, un método multidisciplinario de análisis y evaluación de normas y modelos de gobierno para el ciberespacio.

26. Cuartel General de la Fuerza Aérea de los Estados Unidos, *America's Air Force*, 20.

27. Aerotécnico en el Cuartel General de la Fuerza Aérea, Oficialidad Aérea A6 y A3/6, entrevista no atribuida del autor, 24 de abril de 2014.

28. Uso aquí el término *tunelización* para referirme a la capacidad de acceder a redes IPv6 mediante IPv4 (y viceversa).

29. Sheila Frankel y otros, *Guidelines for the Secure Deployment of IPv6 (Pautas para la implementación segura de IPv6)* (Washington, DC: Instituto Nacional de Normas y Tecnología, 2010), 2-6, http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.

30. Ibíd., 2-7.

31. Entrevistas del autor con líderes superiores, oficiales, personal alistado, ciberoperadores civiles, y no atribuidas, 2013-14.

32. Datos derivados de "Ghost Route Hunter: IPv6 DFP Visibility (Cazador de rutas fantasmas: Visibilidad DFP de IPv6)", SixXS, consultado el 3 de febrero de 2015, http://www.sixxs.net/tools/grh/dfp/.

33. Agradezco a la oficina del AFSN por sus comentarios y colaboración en la producción de esta sección.

34. Para hacer los cálculos, se puede visitar el sitio web del Centro de Integración de Redes del DOD (DODNIC) y realizar una búsqueda "DNIC-RNET [reserve networks]", que encontrará todas las redes que el DODNIC considera "redes devueltas" (el NIC utiliza "RNET" para anotar las redes devueltas a los administradores de IP). Esta información cambia a diario, dependiendo de lo que se emita en cualquier día pero casi siempre disminuye. Véase "Search NIC Whois For", consultado el 3 de febrero de 2015, https://www.nic.mil/cgi-bin/whoisweb.

35. Cuartel General de la Fuerza Aérea de los Estados Unidos, *America's Air Force*, 13.

36. Chad C. Serena y otros, *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network (Lecciones aprendidas de la Red de Misión Afgana: Desarrollo de una red de contingencias de la coalición)* (Santa Mónica, CA: RAND Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR302/RAND_RR302.pdf.

37. Frankel y otros, *Guidelines (Pautas)*, 2-7.

38. *Akamai's State of the Internet* 7 (Estado de Internet según Akamai, 7), no. 1 (Q1 2014): 3, http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf.

39. John P. Stenbit, Oficial Jefe de Información del Departamento de Defensa, a los secretarios de los departamentos militares, memorándum, asunto: Protocolo Internet Versión 6 (IPv6), 9 de junio de 2003, [2], http://www.defense.gov/news/Jun2003/d20030609nii.pdf.

40. Instrucción de la Fuerza Aérea No. 63-101/20-101, *Integrated Life Cycle Management (Administración del ciclo de vida integrado)*, 7 de marzo de 2013, 87, http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101/afi63-101_20-101.pdf.

41. Agradezco al AFNIC/NES por estas observaciones.

42. "Federal Acquisition Regulation; FAR Case 2005–041, Internet Protocol Version 6 (IPv6) (Reglamento de Adquisiciones Federales; FAR Caso 2005-041. Protocolo Internet Versión 6)", en *Federal Register* 74, no. 236 (10 de diciembre de 2009), http://www.gpo.gov/fdsys/pkg/FR-2009-12-10/pdf/E9-28931.pdf.

43. Michael P. Gallaher y Brent Rowe, *Planning Report 05-2, IPv6 Economic Impact Assessment (Informe de planificación 05-2, Evaluación del impacto económico de IPv6)* (Washington, DC: NIST, Departamento de Comercio de los Estados Unidos, Administración de Tecnologías, octubre de 2005), 4-5, http://www.nist.gov/director/planning/upload/report05-2.pdf.

44. John Postel, *NCP/TCP Transition Plan (Plan de transición de NCP/TCP)*, noviembre 1981, 1, https://www.ietf.org/rfc/rfc801.txt.

45. Ibíd., 2.

46. Vivek Kundra, CIO federal, Oficina de Presupuesto y Administración de la Casa Blanca, a los CIO de los departamentos ejecutivos y agencias, memorándum, asunto: Transición a IPv6, 28 de septiembre de 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf.

47. Oficial Jefe de Información del Departamento de Defensa, *Joint Information Environment Implementation Guidelines (Pautas para la implementación del entorno de información conjunto)* (Washington, DC: Oficial Jefe de Información del Departamento de Defensa, 12 de septiembre de 2013), 7, http://dodcio.defense.gov/Portals/0/Documents/JIE/20130926_Joint%20Information%20Environment%20Implementation%20Guidance_DoD%20CIO_Final_Document.pdf.

48. Ibíd., 9.

49. Intercambio de correo electrónico entre el autor y el Cuartel General de la Fuerza Aérea A3/6, 24 de abril de 2014.

Dr. Panayotis A. Yannakogeorgos, PhD (ALB, Harvard University; MS, PhD, Rutgers University) es un profesor investigador de política del ciberespacio del Instituto de Investigación de la Fuerza Aérea de los Estados Unidos (AFRI), Universidad del Aire, Maxwell AFB, Alabama. Su especialidad incluye la intersección del poderío en el ciberespacio, seguridad nacional y operaciones militares; política internacional del ciberespacio; control de armas en el ciberespacio; normas globales del ciberespacio; y seguridad del Mediterráneo Oriental. Anteriormente fue miembro del profesorado en la División de Asuntos Globales de la Universidad Rutgers y consejero en asuntos del Oriente Medio, incluyendo Irán, para el Consejo de Seguridad.