

# Creando un Comando Nuevo en el Ciberespacio

GENERAL KEITH B. ALEXANDER, USA\*

**Nota del Editor:** En marzo de 2011, el General Keith B. Alexander hizo declaraciones ante el Comité de Servicios Armados de la Cámara de Representantes sobre Amenazas Emergentes y Capacidades y el progreso en establecer el Comando Cibernético de EE.UU. Este comentario refleja su declaración en esa ocasión. Este artículo fue publicado anteriormente en nuestra revista *Strategic Studies Quarterly*, Summer 2011.

**L**A CIBERSEGURIDAD es vital para nuestra nación. Parte de nuestra tarea en el Comando Cibernético de Estados Unidos es garantizar que nuestra nación entienda qué es lo que la Casa Blanca, el Congreso y el Departamento de Defensa nos han encomendado y por qué es tan importante que se haga bien. Crear un comando nuevo a la vez que se llevan a cabo las operaciones es un reto, especialmente en tiempos de cambios rápidos tecnológicos y en la política. Pero este comando nuevo ha producido resultados que han hecho que nuestra nación sea más fuerte y segura y ya ha habido dividendos de ciberseguridad en las inversiones de tiempo y recursos dedicados a esta creación.

## El camino hacia la capacidad operacional completa

El Comando Cibernético de EE.UU. logró su capacidad operacional completa (FOC, por sus siglas en inglés) el 31 de octubre de 2010 como un comando sub-unificado bajo el Comando Estratégico de EE.UU. (USSTRATCOM, por sus siglas en inglés). El camino hacia la FOC culminó aproximadamente según el calendario del secretario de defensa cuando él ordenó el establecimiento del comando en junio de 2009. Originalmente se proyectó que la capacidad operacional inicial (IOC, por sus siglas en inglés) se alcanzase en octubre de ese año, pero la fecha se retrasó a mayo de 2010 cuando su nombramiento para desempeñarse como su primer comandante fue confirmado por el Senado. Hicimos buen uso de los meses entre octubre de 2009 y mayo de 2010, sin embargo, crear un estado mayor consolidado para unir las dos organizaciones heredadas, el Comando Conjunto de Componentes Funcionales para la Guerra en la Red (JFCC-NW, por sus siglas en inglés) y la Fuerza de Tarea Conjunta de Operaciones en la Red Global (JTF-GNO), las cuales juntas se convirtieron en el Comando Cibernético. Además, esbozamos las tareas necesarias que nos conducirían a una FOC una vez que el reloj echase a andar. Aunque el intervalo entre la capacidad inicial en mayo y lograr la capacidad operacional completa en octubre fue de solamente cinco meses en lugar de los 12 que se habían planificado, pudimos alcanzar varias metas. Además, lo hicimos acelerando el ritmo de las operaciones diarias que la JTF-GNO y la JFCC-NW habían establecido.

A pesar del horario comprimido, el estado mayor consolidado en el Comando Cibernético logró mucho para octubre de 2010. Establecimos un centro de operaciones conjuntas, transferimos control operacional de la misión de la JTF-GNO al Fuerte Meade, Maryland, y desactivamos el centro de vigilancia 24/7 de la JTF-GNO en Arlington, Virginia; estas medidas ayudaron al USSTRATCOM a disolver la JFCC-NW y la JTF-GNO. La última tarea tomó una cantidad consi-

---

\*El General Keith B. Alexander, Ejército de los EUA, es el Comandante del Comando Cibernético de Estados Unidos, Director de la Agencia de Seguridad Nacional, y Jefe del Servicio de Seguridad Central

derable de tiempo planificarla y una orquestación cuidadosa porque las actividades y la fuerza laboral de la JTF-GNO había que trasladarlas del norte de Virginia al Fuerte Meade, a la vez que se garantizaba que el funcionamiento diario de las redes de información del DoD se mantenían intactas. Establecimos procesos eficaces de mando y control operacional para los conjuntos de misiones consolidadas. Se estableció un centro conjunto de operaciones de inteligencia. Los componentes cibernéticos de nuestro servicio fueron asignados oficialmente al USSTRATCOM, y continuamos forjando relaciones con socios claves. Integramos oficiales de enlace en los comandos combatientes y establecimos las condiciones para ampliar su presencia en elementos de apoyo cibernético más grandes. Desplazamos equipos expedicionarios para apoyar las operaciones en Irak y Afganistán. Además, logramos progresar en nuestro apoyo a la planificación operacional por parte de los comandantes combatientes y en crear procesos para que ellos emitieran requerimientos de apoyo cibernético. El comando logró todo esto sin impactos negativos a la misión, manteniendo seguras las operaciones del departamento a la vez que hacía transparente la transición a los usuarios de sus sistemas informáticos.

Se proyecta que el presupuesto del comando para el año fiscal 2012 sea de \$159 millones de dólares, y se espera que para ese entonces la fuerza laboral sea de 464 efectivos y 467 civiles, un total de 931 empleados. La misión general de este equipo es planificar, coordinar, integrar, sincronizar y conducir actividades para dirigir las operaciones en la defensa de redes de información específicas del DoD y estar preparado, cuando se le ordene, para llevar a cabo el espectro total de las operaciones militares ciberespaciales con el fin de habilitar las acciones en todos los ámbitos, garantizar la libertad de acción en el ciberespacio para EE.UU. y sus aliados y negarle lo mismo a nuestros adversarios. Por último, el Comando Cibernético de EE.UU. continúa creando sinergia con la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) con el fin de aprovecharse de la infraestructura y experiencia de la NSA, que continúan siendo cruciales para nuestro progreso. Nuestra coubicación con la NSA le permite al gobierno maximizar nuestros talentos y capacidades colectivas.

## Perspectivas actuales

Nuestros líderes, desde el Presidente Obama y sucesivamente, han hablado sobre la importancia para nuestra nación de conservar nuestra seguridad en el ciberespacio y mantener nuestra libertad de acción en este ámbito nuevo, singular y fabricado por el hombre. Al hacerlo enfrentamos muchos retos, especialmente en virtud de los últimos acontecimientos.

La amenaza cibernética continúa evolucionando, constituyendo peligros que sobrepasan las fallas en el 2008 de nuestros sistemas clasificados que el Subsecretario de Defensa, William Lynn, describió en su artículo en la revista *Foreign Affairs* en el otoño de 2010 como un momento decisivo para nuestra seguridad cibernética. Ahora, nuestra nación depende del acceso al ciberespacio y los datos y capacidades que radican ahí; somos colectivamente vulnerables a una gama de amenazas que van desde inestabilidad en la red, actividades criminales y terroristas, hasta capacidades auspiciadas por el estado que están progresando desde explotación a interrupción a destrucción. Si bien no hemos sufrido daños desastrosos o irreparables en el ciberespacio de ninguna de esas categorías de riesgo, debemos estar preparados para contrarrestar esas amenazas.

Tanto los actores externos como las amenazas internas constituyen retos significativos para nuestra ciberseguridad. Por supuesto, ningún actor estatal ha admitido haber lanzado ciberataques perjudiciales a otro estado. Sin embargo, han ocurrido incidentes que se asemejan mucho a esos ataques. Los ciberasaltos en Estonia en el 2007 incitaron a Estados Unidos y nuestros aliados de la OTAN a reflexionar sobre qué constituiría un “ataque armado” en el ciberespacio a un miembro de la alianza que provocase las provisiones del Tratado del Atlántico Norte sobre la defensa colectiva. El año siguiente, la invasión de Georgia coincidió con ciberataques planificados con precisión, marcando una de las primeras veces que hemos visto esos “ataques apoyados

por la cibernética”. La coincidencia fue tan perfecta que observadores independientes llegaron a la conclusión de que no hubo tal coincidencia—que los piratas informáticos (*hackers*) que habían imposibilitado temporalmente la reacción y las comunicaciones del gobierno georgiano con el mundo exterior habían practicado sus asaltos y respondieron a indicios oficiales cuando los montaron de verdad.

Recientemente hemos visto el acceso a la *Internet* manipulado o restringido por los gobiernos para contener e interrumpir hasta las protestas pacíficas de sus propios ciudadanos. Además, creemos que los actores estatales han creado armamento cibernético para paralizar los blancos de la infraestructura en maneras equivalentes a asaltos cinéticos; algunos de esos armamentos podrían posiblemente destruir *hardware* al igual que datos y *software*. Las posibilidades de efectos cibernéticos destructivos, hace tiempo reconocidos como teóricos en su mayoría, ahora se han producido afuera del laboratorio y se están proliferando hacia los arsenales nacionales y posiblemente más allá, moviéndolos un paso más cerca al uso intencional o la liberación accidental. Segmentos de la infraestructura crítica de nuestra nación no están preparados para lidiar con este tipo de amenaza.

Además, contemplamos con inquietud las capacidades cada vez mayores de los actores no estatales. Las amenazas que vemos aquí son asimétricas, lo que significa que actores comparativamente nuevos o menores pueden causar efectos acordes con acciones auspiciadas por el estado. Aunque individuos con destrezas en computación han mostrado independientemente que esos ataques los puede lanzar un solo actor con una computadora portátil y un motivo, estamos enfocados principalmente en terroristas y criminales cibernéticos bien organizados. Éstos continúan tornándose más hábiles para usar la *Internet* como un medio para reclutar, coordinar y llevar a cabo otras actividades, y cada vez se tornan más sofisticados al hacerlo. Los criminales cibernéticos están más interesados en robar y sacarle provecho a información sensitiva que pueden darles ganancias, ya sea directamente a través del fraude o robo de identidad o indirectamente a través de la piratería de capital intelectual. De hecho, el verano pasado observadores tales como el Senador Sheldon Whitehouse y un grupo de colegas bipartitas le llamaron a esto “la transferencia de riqueza más grande en la historia de la humanidad a través del robo y la piratería”—una transferencia que significativamente ha reducido el costo para que posibles adversarios cierren y contrarresten nuestra ventaja tecnológica. Por supuesto, esa actividad es un delito y pertenece más correctamente a la policía que a los militares, pero cuando el blanco principal es nuestra base industrial de defensa, nosotros en el Departamento de Defensa tenemos que desempeñar un papel en la respuesta. También sabemos que actores estatales y terroristas pueden sacarle provecho a las infracciones y herramientas fabricadas por criminales, al igual que un agente patógeno peligroso emplea, de manera oportunista, un vector de enfermedades para penetrar las células huésped. De hecho, a veces los actores estatales y no estatales colaboran en asuntos de interés mutuo.

Retos de seguridad significativos también emanan de la higiene cibernética deficiente, mal uso inadvertido y actos maliciosos. Después de todo, incluso el más astuto de los actores cibernéticos maliciosos—aquellos que pueden entrar en prácticamente cualquier red a la que en realidad quieren intentar penetrar—por lo regular están buscando blancos de oportunidad. Ellos buscan vulnerabilidades fáciles en la seguridad de nuestro sistema y luego se aprovechan de ellas. Parches de *software* que no se han aplicado, *firewalls* desatendidas y *suites* de antivirus que nunca se actualizan inclusive en la milicia estadounidense, nos causan problemas graves, especialmente cuando un riesgo para uno es un riesgo compartido por todos. Ahora, multiplique esos problemas a lo largo del gobierno y del sector privado, y comprenda que hemos interconectado nuestras vulnerabilidades a la vez que hemos segmentado nuestras defensas entre los ámbitos .mil, .gov, .com, .edu de la *Internet*. Cada ámbito (y a menudo cada sistema) ha sido abandonado para que se las arregle como pueda contra actores cibernéticos que no están interesados

en distinciones jurídicas o límites organizacionales. Y, por último, hay una amenaza interna; algunas de las violaciones de seguridad más grandes en la historia han originado desde adentro.

La creación reciente del Comando Cibernético se ha granjeado mucho interés por parte de militares extranjeros y los gobiernos que los supervisan. Con frecuencia vemos informes de prensa sobre países que están contemplando crear sus propios “comandos cibernéticos”. Esto parece ser una señal no necesariamente de una “militarización” del ciberespacio sino más bien un reflejo del nivel de inquietud con la que líderes civiles y militares alrededor del mundo contemplan los problemas actuales. Muchos de esos pasos son esencialmente defensivos, y si tantos países están interesados en mejorar sus defensas, estarían más dispuestos a discutir sobre las maneras como pueden disminuir las amenazas comunes. Al nivel estratégico del ciberespacio hay una disuasión *de facto* peligrosa. Aunque nadie sabe cómo se desarrollaría una ciberguerra, hasta los actores estatales más capaces parecen reconocer que no está en el interés de nadie enterarse a la mala. Esta inquietud ha provocado cierto grado de restricción por estados que consideramos son capaces de ocasionar efectos cibernéticos muy graves. A menos que el optimismo oculte las amenazas verdaderas, debemos destacar que no contamos con una capacidad segura de refrenar el comportamiento de extremistas radicales, no estatales.

En resumen, nuestros adversarios en el ciberespacio son sumamente capaces. Nuestra economía y sociedad se han tornado dependientes, directa o indirectamente, en el acceso a y la libertad de movimiento en el ciberespacio—y de hecho nuestra milicia depende igual de ese acceso—y, por lo tanto, no podemos estar a gusto con una situación en la cual a veces somos nuestro peor enemigo.

## Trabajando hacia el futuro

La finalidad de los esfuerzos y la planificación del Comando Cibernético de EE.UU. es garantizar que el DoD ha hecho todo lo que puede para defenderse en contra de y disuadir adversarios, mitigar amenazas peligrosas y tratar las vulnerabilidades persistentes de manera que inclusive nuestros opositores más capaces sabrán que interferir con las propiedades de nuestra nación en el ciberespacio es una mala inversión.

Nuestro comando enfrenta serios retos a medida que se prepara para llevar a cabo trabajos en el ciberespacio que se necesitan urgentemente. Su establecimiento refleja la necesidad del departamento de administrar los riesgos cibernéticos, asegurar la libertad de acción y garantizar el desarrollo de capacidades integradas. Nuestra intención es superar los retos que enfrentamos mediante los esfuerzos concertados de implementar la recién aprobada estrategia para el ciberespacio del departamento. Continuaremos buscando la solución a los problemas de capacidad, recursos y eficiencias de la tecnología de informática que enfrentamos mediante las cinco iniciativas estratégicas de esa estrategia. Nuestra intención es:

- tratar el ciberespacio como un ámbito para fines de organizar, capacitar y equipar, de manera que el DoD pueda aprovechar completamente su potencial en las operaciones militares, de inteligencia y de negocios;
- emplear nuevos conceptos operacionales de defensa, inclusive ciberdefensas activas tales como vigilar la seguridad del tráfico de los sistemas de informática, hasta proteger las redes y los sistemas del DoD;
- colaborar de cerca con otras agencias y departamentos del gobierno de EE.UU. y el sector privado para permitir una estrategia integral por parte del gobierno y un método nacional integrado hacia la ciberseguridad;
- forjar relaciones robustas con los aliados y socios internacionales de Estados Unidos para permitir que se comparta la información y se fortalezca la ciberseguridad colectiva; y

- sacarle provecho a la ingeniosidad de la nación reclutando y reteniendo una fuerza laboral cibernética excepcional y dar lugar a la innovación tecnológica rápida.

Nuestro primer deber es garantizar que las redes del DoD estén seguras. Hacerlo es crítico para proteger nuestros datos, mantener nuestro potencial bélico y en un final defender nuestra nación. Hasta hace poco, todos opinábamos que nuestras redes eran un gran multiplicador de fuerza—la magia que nos permite colocar pertrechos en el blanco y enviar aeronaves, tropas y buques a donde se necesitaban, cuando tenían que estar ahí. Sin embargo, hoy comprendemos que esas redes representan una vulnerabilidad grave y tememos a la idea que alguien logre destruirlas o, peor aún, haga unos cuantos cambios sutiles a la integridad de nuestros datos de manera que paralizaría todas nuestras operaciones militares. Sin el flujo de datos rápido, garantizado y seguro no podremos combatir nuestros adversarios en la manera como nosotros, en calidad de estadounidenses, pensamos que se deben combatir. No estamos necesariamente cerca de perder esa ventaja, pero los posibles adversarios comprenden dónde radica y, de hecho, están contemplando maneras de debilitarla en cualquier conflicto en el futuro.

El Comando Cibernético de EE.UU. está trabajando de muchas maneras para conservar esa ventaja de información. Estamos dirigiendo las operaciones de las redes de informática del departamento, que unen siete millones de dispositivos de computadoras a lo largo de quince mil redes. El reciente traslado de la Agencia de los Sistemas de Información de la Defensa (DISA, por sus siglas en inglés) a una nueva instalación en el Fuerte Meade ha dado lugar a una mayor colaboración entre nuestras dos organizaciones. Esa labor incluye el mantenimiento de sensores para detectar y bloquear la actividad del adversario en esas redes, la inspección de ámbitos y prácticas de seguridad y la investigación de incidentes reales o sospechosos. Juntas estamos progresando en todas esas áreas, fomentando nuestra capacidad para detener intromisiones y adaptarnos a los cambios en las prácticas casi tan rápido como evolucionan. Las capacidades de sensor nuevas que estamos desplazando y el régimen de inspección dinámico que estamos preparando mejorarán aún más nuestra situación.

También planificamos—en asociación con la NSA—la defensa de sistemas de información específicos del DoD, a sabiendas de que tenemos que mantenernos a la delantera de la amenaza cibernética en términos tecnológicos. En este aspecto, el Comando Cibernético de EE.UU. y nuestros socios están buscando maneras de cambiar a una arquitectura diferente y más defendible para ofrecer servicios de informática a los usuarios. De aquí a un año debemos estar bien encaminados en contar con una arquitectura templada comprobada, desplazada y que ofrece un nivel nuevo de ciberseguridad. La idea es reducir las vulnerabilidades innatas en la arquitectura actual y aprovechar las ventajas de *“cloud” computing* (computación en nube) y redes *thin-client* (estrechas), moviendo los programas y los datos que los usuarios necesitan lejos de los miles de computadoras de mesa que ahora usamos—cada una de las cuales hay que asegurar individualmente—a una configuración centralizada que nos otorgue una disponibilidad de ampliaciones más amplia y datos combinados con un control más estricto en cuanto a accesos y vulnerabilidades y más mitigación oportuna de estas últimas. Cambiar a una arquitectura *cloud* tiene las ventajas de producir economías de escala y reducir los costos de la tecnología de información del departamento. Además, a primera vista pareciera que esta arquitectura es vulnerable a las amenazas internas—de hecho, ningún sistema que los seres humanos usan está inmune al abuso—pero estamos convencidos que los controles y herramientas que se incorporen al *cloud* garantizarán que las personas no podrán ver ningún dato más allá de los que necesitan para sus trabajos y se les identificará rápidamente si intentan el acceso no autorizado a los datos.

Durante el año próximo esperamos “poner en marcha” las redes de nuestro departamento. Desde luego, continuaremos haciéndolo respetando plenamente y protegiendo la privacidad y las libertades civiles de todos los estadounidenses, al igual que en cumplimiento con todas las leyes y regulaciones pertinentes. La idea es transformar los sistemas de información del DoD de

algo que es protegido pasivamente a un conjunto de capacidades que les ofrece a nuestros comandantes y líderes superiores oportunidades para ajustar nuestras defensas. Si aquellos que buscan hacernos daño en el ciberespacio aprenden que hacerlo es costoso y difícil, creemos que sus patrones de conducta cambiarán. La tecnología está preparada.

En el documento de misión de nuestro comando se declara que coordinamos, integramos y sincronizamos actividades para dirigir las operaciones y la defensa de las redes de DoD. En práctica, esto significa que invertimos mucho tiempo hablando con los líderes y expertos en el departamento, el gobierno estadounidense, la industria privada al igual que con otros países. Por supuesto, este esfuerzo comienza con los componentes de servicio cibernético del Comando Cibernético de EE.UU., que proveen las fuerzas que implementan nuestros planes y ejecutan nuestras directrices—Comando Cibernético del Ejército, Comando Cibernético de las Fuerzas de Infantería de Marina, Comando Cibernético de la Flota y el Comando Cibernético de la Fuerza Aérea. Aún estamos perfeccionando las maneras como nosotros y ellos interactuaremos para apoyar y ser apoyados por los comandos combatientes geográficos en distintas situaciones. Nuestra misión también depende de la labor de la NSA, que provee inteligencia y experiencia que son indispensables para comprender lo que está sucediendo en el ciberespacio. Además, estamos constantemente comprometidos con DISA y nuestra relación con esta agencia probablemente cambiará sustancialmente y cada vez será más estrecha en el futuro cercano.

También hemos fortalecido nuestra asociación con el Departamento de Seguridad Interna (DHS, por sus siglas en inglés) según el acuerdo reciente celebrado por los Secretarios Robert Gates y Janet Napolitano. Un funcionario superior de DHS ahora trabaja con nosotros en la NSA, está al frente de un elemento de coordinación conjunta DHS-DoD que también fue establecido por el acuerdo y asiste a muchas de las reuniones de los líderes. Varias agencias gubernamentales también son representadas 24 horas al día en nuestro centro de operaciones conjuntas. Esas medidas, junto con las medidas complementarias en el DHS y otros socios, deben proporcionar una concienciación en todo el gobierno de lo que todos pueden apreciar de manera que podamos planificar y ejecutar acciones conjuntas autorizadas y coordinadas en caso de una emergencia. Por último, somos participantes activos en las discusiones productivas del Departamento de Defensa entre el gobierno y la industria sobre cómo compartir información relacionada con las amenazas comunes y las posibles maneras de mitigarlas. La gran mayoría de la información de nuestra milicia viaja en infraestructura comercial, y por lo tanto necesitamos crear discernimientos compartidos en esas dependencias para fines de asegurar la misión.

La segunda parte de nuestra misión en el Comando Cibernético es estar preparados para llevar a cabo operaciones militares ciberespaciales de todo tipo. Como mencioné anteriormente, los actores estatales y no estatales ya han experimentado con maneras de hostigar o atacar gobiernos rivales, ya sea para plantear un punto estratégico o en combinación con ataques cinéticos. Sería desacertado que nuestra milicia y nuestra nación diesen por sentado que hemos visto los últimos de esos ataques. Estamos preparados, cuando se nos ordene y en cumplimiento total con las leyes pertinentes, a responder cuando nosotros o nuestros aliados seamos amenazados o sometidos al uso de la fuerza en el ciberespacio. El Presidente ha recalcado que nuestra infraestructura digital es un recurso nacional estratégico y ha insistido que preparar a nuestro gobierno para la tarea de proteger los recursos nacionales estratégicos en el ciberespacio es una prioridad de seguridad nacional. Nuestros esfuerzos para hacerlo están concebidos para lograr dos metas:

- Primero, protegemos en el ciberespacio la libertad de acción de EE.U. y los aliados. Ya no es posible concebir que nuestra nación funcione correctamente o inclusive se defienda sin la capacidad de crear, transmitir y asegurar montones de datos digitalizados. Hacer imposible, o siquiera problemático, nuestro acceso al ciberespacio representaría una amenaza estratégica a los intereses vitales de Estados Unidos—uno que a nuestro comando se le ha establecido y encomendado evitar con respecto a las operaciones del DoD en el ciberespacio.

Además, nuestra seguridad cibernética está inextricablemente unida con la de nuestros aliados, y nuestros intereses en el ciberespacio también pueden coincidir con aquellos de otros estados con los cuales tenemos lazos menos formales. La falta de fronteras geográficas en el ciberespacio significa que una amenaza a uno puede constituir una amenaza a todos, lo que nos ofrece un incentivo verdadero para compartir concienciación situacional y las mejores prácticas que ayuden a proteger a nuestra milicia, gobierno y redes privadas y datos.

- Segundo, cuando se nos ordene, necesitamos negarles a nuestros adversarios la libertad de acción en el ciberespacio. Al igual que con todas las actividades que el DoD emprende, las operaciones solamente se ejecutan con una misión clara y bajo autoridades claras, y son gobernadas por todas las leyes pertinentes, inclusive la ley del conflicto armado. No nos podemos dar el lujo de permitir que el ciberespacio sea un santuario en el que adversarios reales y posibles puedan organizar fuerzas y capacidades para usarlas contra nosotros y nuestros aliados. Este no es un peligro hipotético; en las zonas de conflicto donde las fuerzas estadounidenses están trabadas en combate hemos visto, de hecho, que la *Internet* se emplea para reclutar, recaudar fondos, adiestramiento operacional y otras actividades dirigidas en contra del personal de nuestro servicio y los socios de la coalición. En el Comando Cibernético gran parte del enfoque está en ayudar a nuestras tropas en campaña a que limiten las vulnerabilidades en y desde el ciberespacio. Este esfuerzo refleja la probabilidad de que, a partir de ahora, todos los conflictos tendrán un aspecto cibernético, y nuestros intentos para comprender esta evolución serán cruciales para la seguridad futura de Estados Unidos.

## Conclusión

El Departamento de Defensa dio un paso importante para nuestra nación al crear el Comando Cibernético de EE.UU. y declararlo completamente operacional. En el Comando Cibernético tenemos una misión de administrar activamente las redes de información del departamento—no solo defenderlas sino también utilizarlas como una herramienta conservando su libertad de acción—y estar igual de preparados para utilizar nuestras capacidades para interrumpir cualquier uso del ciberespacio por parte de nuestros enemigos en contra de los intereses de Estados Unidos. El comando busca:

- aumentar la capacidad de la fuerza laboral cibernética;
- implementar y sacarle provecho, en una asociación sólida con la NSA, la transformación de las redes del departamento;
- trabajar con los comandos combatientes para sincronizar procesos y planificar para entregarles los efectos conjuntos que requieren;
- extender las capacidades de defensa cibernética a lo largo de las redes del gobierno de EE.UU. a través del apoyo de asociaciones con la NSA y el DHS a medida que se esfuerza por asegurar los sistemas de seguridad federales, civiles y no nacionales y,
- con el DHS, incrementar el diálogo del gobierno con los socios privados en cuanto a la protección de la infraestructura crítica de nuestra nación.

El Comando Cibernético de Estados Unidos funciona respetando las libertades civiles y en cumplimiento con las leyes que rigen la privacidad de nuestros compatriotas y según las directrices de la autoridad de mando nacional, y en combinación con los socios de misión en los Departamentos de Defensa, Seguridad Interna, la policía, la comunidad de inteligencia, la industria y el mundo académico. Nosotros no consideramos la seguridad de nuestra nación y la protección de las libertades civiles y la privacidad como un “equilibrio”, más bien, creemos que debemos defender ambas. Confío que juntos tendremos éxito. ■