Política para la seguridad cibernética de EUA

Teniente Coronel August G. Roesener, PhD, USAF
Mayor Carl Bottolfson, USAF
Capitán de Fragata Gerry Fernández, USN

Desde la creación de la primera red de computadoras interconectada en 1969 como una iniciativa de la Agencia de Proyectos de Investigación Avanzada, el espacio cibernético se ha ampliado para afectar muchos, o casi la mayoría, de los aspectos de las vidas de los estadounidenses. Lamentablemente, el acceso a y la expansión de la *Internet* a menudo han continuado sin la consideración correcta por la seguridad de la información contenida o transmitida en ella. La falta de la seguridad necesaria y el anonimato que ofrece la *Internet* condujo a un crecimiento igualmente rápido (sino mayor) de la vil explotación de este ámbito creado por el hombre. Desgraciadamente, es poco probable que "Estados Unidos pueda proteger la creciente amenaza de los delitos cibernéticos y las intrusiones y operaciones auspiciadas por estados".[1] Sin embargo, esta posibilidad no debe limitar los intentos de Estados Unidos de defender su infraestructura ciberespacial, "ya sea que la amenaza venga de terroristas, delincuentes cibernéticos o estados y sus representantes".[2] Por consiguiente, Estados Unidos debe crear capacidades cibernéticas de ofensiva y defensiva. Además, las políticas claramente definidas exigen desarrollo e implementación para garantizar la cohesión a lo largo de todo el gobierno. Con respecto a los ataques en el ámbito cibernético a los sistemas civiles de EUA que se atribuyen a una nación estado, el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) debe tener la responsabilidad de responder (en la forma de gestión de las consecuencias); el Comando Norte de EUA (USNORTHCOM, por sus siglas en inglés), la evaluación de ataques internos; y el Comando Cibernético de EE.UU. (USCYBERCOM, por sus siglas en inglés) la defensa y cualquier respuesta de contraataque (en coordinación con los comandos combatientes pertinentes y las agencias nacionales estadounidenses). En este artículo se describen el entorno del espacio cibernético y sus amenazas; se explican las autoridades, funciones y responsabilidades actuales de estas y otras agencias y se detalla cómo esas autoridades, funciones y responsabilidades necesitan modificarse para proteger de la mejor manera los intereses de seguridad nacional de Estados Unidos.

El entorno

El espacio cibernético es "la infraestructura de información digital y comunicaciones interconectada globalmente".[3] Desde los teléfonos inteligentes con sistemas de navegación, la banca en línea y las comunicaciones globales, el espacio cibernético es una porción esencial de las vidas de la mayoría de los estadounidenses. El Departamento de Defensa de EUA (DOD, por sus siglas en inglés) decidió recientemente "tratar al espacio cibernético como un ámbito operacional".[4] En vista de la facilidad y el costo relativamente bajo de llevar a cabo operaciones en el espacio cibernético (en comparación con los ámbitos físicos de aire, tierra, mar y espacio), al igual que la anonimidad provista por este ámbito virtual, las amenazas y los ataques cibernéticos son más predominantes y se puede decir que son igual de peligrosos que aquellos en los ámbitos físicos. De hecho, en la Estrategia de Seguridad Nacional del 2010 se destaca que "las amenazas a la seguridad cibernética representan uno de los retos más graves a la seguridad nacional, a la seguridad pública y a la economía que enfrentamos como nación".[5] Esta declaración es particularmente alarmante porque "las operaciones extranjeras en el espacio cibernético en contra de los

sistemas en el sector público y privado de Estados Unidos están aumentando en cifras y complejidad. Las redes del DoD son investigadas millones de veces todos los días".[6] Aunque no se manifiestan fácilmente, esos ataques pudiesen afectar las vidas de los ciudadanos estadounidenses corrientes. De hecho, esos tipos de amenazas y ataques cibernéticos "van más allá de los blancos militares y afectan todos los aspectos de la sociedad estadounidense. En vista de la naturaleza integrada del espacio cibernético, las fallas inducidas por computadora a las redes eléctrica, de transporte y a los sistemas financieros podrían ocasionar daños físicos masivos y la interrupción económica".[7] El posible impacto negativo en los intereses nacionales de EUA, al igual que a las vidas y activos de los ciudadanos estadounidenses, exigen la preparación y protección del gobierno en el ámbito virtual igual a aquellos en los ámbitos físicos.

Autoridades, funciones y responsabilidades

A continuación, se explican las autoridades, funciones y responsabilidades actuales para asegurar y defender el espacio cibernético, analizando aquellas del sector privado y luego su relación con las agencias gubernamentales de EE.UU. —específicamente, el Departamento de Comercio (DOC), DHS, el Departamento de Justicia (DOJ), el Departamento de Energía (DOE) y el DOD, incluyendo el Comando Estratégico de EUA (USSTRATCOM), USCYBERCOM, USNORTHCOM y la Agencia de Seguridad Nacional (NSA). Aquí, *sector privado*, tiene que ver con cualquier entidad estadounidense no gubernamental— un individuo, una compañía pequeña o una corporación grande. En vista de que datos e información con posibles intereses vitales de seguridad nacional y económicos radican en las redes del sector privado, son blancos para las violaciones cibernéticas en la forma de espionaje de nación estado y corporativo, robo de identidad, terrorismo económico y así sucesivamente. En virtud de los problemas de la privacidad inherente en la protección y defensa del espacio cibernético del gobierno de Estados Unidos, coloca pocos requisitos en el sector privado para reportar intrusiones o ataques cibernéticos. En la Directiva Presidencial 21, la administración Obama designó al DOC, en colaboración con el DHS y otros departamentos y agencias federales relevantes, como la agencia principal para "involucrar a las organizaciones en el sector privado, de investigación, académicas y gubernamentales a que mejoren la seguridad para la tecnología y las herramientas necesarias para los sistemas basados en la cibernética".[8] La meta de esta iniciativa incluye la colaboración para realzar la protección y la seguridad pero involucrando solamente actividades de *participación*. El DOC no cuenta con la autoridad ni para exigir ni hacer cumplir los estándares de la seguridad cibernética en esas instituciones.

Otros actores claves en el sector privado, tales como la base industrial de la defensa (DIB, por sus siglas en inglés), cuentan con acceso a o supervisan aspectos de interés nacional y por lo tanto reciben más énfasis en la seguridad cibernética. La DIB incluye "las organizaciones y corporaciones públicas y privadas que apoyan al DoD mediante el suministro de tecnologías de defensa, sistemas de armamento, desarrollo de política y estrategia y personal".[9] En un memorándum a los líderes del DOD, el subsecretario de defensa destacó que "las amenazas cibernéticas a los sistemas de informática no clasificados de la DIB representan un riesgo inaceptable de comprometer la información del DOD y constituyen una amenaza inminente a la seguridad nacional y a los intereses económicos de EUA."[10] Por consiguiente, el DOD implementó un programa de garantía de seguridad cibernética y de información en la que "el DOD le ofrece a las compañías DIB información clasificada y no clasificada de amenazas cibernéticas y las mejores prácticas de garantía de información".[11] Entonces, las agencias DIB tienen la responsabilidad de "reportar incidentes cibernéticos que puede que incluyan información del DOD para su análisis, desarrollo de estrategias coordinadas de mitigación y, cuando se necesiten, evaluación de daños de intrusiones cibernéticas de información del DOD que haya sido comprometida".[12] Lamentablemente, el hecho de que esta "responsabilidad" no es un requisito sino voluntario disminuye la

probabilidad de que el actor DIB se auto reportará porque, una vez catalogada como una inquietud de seguridad, podría perder contratos con el gobierno y por ende reducir las ganancias.

Además de la DIB, el gobierno estadounidense conserva un interés particular en proteger a las agencias que controlan porciones de la infraestructura crítica y recursos claves (CIKR, por sus siglas en inglés) de Estados Unidos, incluyendo "sistemas y recursos, ya sean físicos o virtuales, tan vitales que incapacitarlos o destruirlos podría tener un impacto debilitante en la seguridad, economía, salud pública o seguridad, medio ambiente, o cualquier combinación de ellos".[13] Los recursos claves de EUA son "recursos controlados pública o privadamente que son esenciales para las operaciones mínimas de la economía y del gobierno".[14] Para aumentar la seguridad cibernética y la concienciación, a los dueños y operadores de la CIKR se les *exhorta* que permanezcan "integrados física y virtualmente en el Centro Nacional de Integración de Comunicaciones y Seguridad Cibernética (NCCIC, por sus siglas en inglés) del DHS durante operaciones de estado estacionario y completa y correctamente integradas en las capacidades de respuesta a incidentes cibernéticos".[15] Nuevamente, en vista de que este es el sector privado, cualquier participación es puramente voluntaria. Además, el Presidente Obama emitió una Orden Ejecutiva sobre la Mejora de la Infraestructura Crítica de la Seguridad Cibernética en la que se destaca que "para poder maximizar la utilidad de compartir información sobre amenazas cibernéticas con el sector privado, el Secretario (de Seguridad Nacional) ampliará el uso de programas que incluyan en el servicio federal de manera temporal a expertos en la materia del sector privado".[16] Por consiguiente, esos expertos pueden "ofrecer asesoramiento con respecto al contenido, estructura y tipos de información más útiles para propietarios y operadores en reducir y mitigar riesgos cibernéticos".[17] En vista de que no hay ni asociaciones ni relaciones fuertes entre el sector privado y el gobierno estadounidense en este contexto, los datos y la información en sus redes son vulnerables a los ataques cibernéticos en la forma de intrusión y explotación. Esta vulnerabilidad constituye una gran amenaza para la seguridad nacional de Estados Unidos.

En la Directiva Presidencial Núm. 7 del Departamento de Seguridad Nacional, el Presidente George W. Bush designó al DHS como la agencia principal para la protección de la infraestructura crítica, especificando que el Secretario de Seguridad Nacional "mantendrá una organización para servir como punto de referencia para la seguridad en el espacio cibernético."[18] Estas funciones y responsabilidades reciben detalles adicionales y perfeccionamiento en que "a través del CS&C (seguridad cibernética y comunicaciones), el Secretario de Seguridad Nacional es responsable de ofrecer gestión y coordinación durante una crisis en respuesta a Incidentes Cibernéticos Significativos".[19] Además, en calidad de agencia principal del NCCIC, el DHS

> coordina con todos los socios, inclusive las agencias policiales, encabezando la iniciativa nacional de investigar y enjuiciar los delitos cibernéticos, con la comunidad de inteligencia (IC, por sus siglas en inglés) con respecto a las amenazas, inteligencia y atribución; con elementos del DOD con respecto a la inteligencia, el intercambio de información y las operaciones militares para defender la nación; con los gobiernos estatales y locales y el sector privado para garantizar que se le saca provecho a la concienciación común de la situación operacional por parte de todas las organizaciones de respuesta a medida que ejecutan sus autoridades y misiones individuales.[20]

Con la Directriz Presidencial 21, la administración Obama modificó ligeramente esas misiones declarando que el DHS mantiene la responsabilidad de "coordinar las respuestas del gobierno federal a incidentes cibernéticos o físicos significativos que afectan a la infraestructura crítica".[21] Resulta importante destacar que a pesar de que el DHS está a cargo de la seguridad cibernética, su preocupación principal está en el área de respuesta y gestión en situaciones de crisis y la coordinación con otras agencias. De hecho, el "DHS en la actualidad cuenta con una responsabilidad legal muy limitada para la protección de los sistemas de informática federales".[22] El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), una agencia federal no reglamentaria dentro del DOC, ha establecido un marco de seguridad cibernética

para ayudar "a propietarios y operadores de infraestructura crítica a reducir riesgos en industrias tales como generación de energía, transporte y telecomunicaciones".[23] Por lo tanto, un departamento estadounidense establece los estándares para la seguridad cibernética de la infraestructura crítica y otro está a cargo de proteger esos recursos en el ámbito cibernético. Además, según Mark Weatherford, subsecretario del DHS de seguridad cibernética para la Protección Nacional y Dirección del Programa, "Hay una falta verdadera de talento en seguridad cibernética. Me refiero al verdadero personal tipo ninja en torno al cual crear su programa de seguridad. No creo que sea una exageración decir que esto es una emergencia nacional".[24] La falta de autoridades y capacidades apropiadas le impide al DHS poder cumplir adecuadamente sus responsabilidades definidas.

En la Directriz Presidencial 7 del Departamento de Seguridad Nacional, el Presidente Bush le encomendó al DOJ, incluyendo al Buró Federal de Investigaciones (FBI, por sus siglas en inglés), a "reducir las amenazas terroristas internas e investigar y enjuiciar ataques terroristas actuales o intentados en, el sabotaje de, o las interrupciones de la infraestructura crítica y recursos claves".[25] Aunque esas funciones no mencionan específicamente el espacio cibernético, las del procurador general fueron subsiguientemente perfeccionadas de manera que incluyan ofrecer "asesoramiento sobre asuntos legales que requieren resolución durante esfuerzos para responder a y recuperarse de un incidente cibernético, administrar cualquier delito o investigaciones nacionales de inteligencia extranjera; y compartir información que surja de esas investigaciones según lo permita la ley".[26] Al FBI se le encomendó la responsabilidad de desempeñarse en calidad de la "agencia principal operando internamente para proteger y defender a Estados Unidos en contra de amenazas terroristas y de inteligencia extranjera, inclusive aquellas que cuentan con un nexo cibernético".[27] La Directriz Presidencial 21 modificó esas funciones de manera que el FBI "lleve a cabo recopilación, análisis y diseminación interna de información de amenazas cibernéticas".[28] Además, el FBI opera la Fuerza Nacional de Tarea Conjunta de Investigación Cibernética —el "punto central para todas las agencias gubernamentales para coordinar, integrar y compartir información relacionada con todas las investigaciones internas de amenaza cibernética,. . . tornando la Internet más segura persiguiendo a terroristas, espías y delincuentes que buscan explotar los sistemas (de Estados Unidos)".[29] Algunas funciones incluyen inquietudes sobre el espacio cibernético, pero la responsabilidad del DOJ radica principalmente en la prevención de actividades terroristas en el espacio cibernético al igual que investigar y enjuiciar a aquellos que cometen ese tipo de actividades.

La seguridad cibernética es una inquietud de suma importancia para el DOE porque "se puede decir que una red eléctrica resistente es la infraestructura más compleja y crítica en la cual otros sectores dependen para ofrecer servicios esenciales".[30] Según el NIST, la seguridad cibernética "se debe incluir en todas las fases del ciclo de vida del sistema (eléctrico), desde la fase de desarrollo hasta la implementación, mantenimiento y disposición".[31] El DOE apoya la seguridad cibernética para la red eléctrica "facilitando asociaciones públicas-privadas para acelerar las iniciativas de seguridad cibernética para el siglo XXI; financiar la investigación y el desarrollo de la tecnología avanzada para crear una infraestructura de electricidad resistente y apoyar el desarrollo de estándares de seguridad cibernética para ofrecer una línea de base para proteger contra vulnerabilidades conocidas".[32] Por lo tanto, el DOC (a través del NIST) establece los estándares para la seguridad cibernética de la infraestructura crítica; el DHS protege la infraestructura crítica en el ámbito cibernético y el DOE es dueño de una porción grande de la infraestructura crítica del gobierno de Estados Unidos. Este arreglo inevitablemente produce ineficiencias con la seguridad cibernética para estos recursos.

En calidad de agencia principal responsable de la defensa nacional, el DOD mantiene funciones y responsabilidades claves en el espacio cibernético. Depende en gran medida del espacio cibernético, de hecho, "el DOD utiliza el espacio cibernético para permitir sus operaciones militares, de inteligencia y comerciales, inclusive el movimiento de personal y material y el comando

y control del espectro total de las operaciones militares".[33] Por consiguiente, el departamento depende mucho de sus redes para el "comando y control de sus fuerzas, de la inteligencia y la logística de las cuales depende y de las tecnologías de armamento que diseñamos y ponemos en servicio".[34] El ámbito virtual, por lo tanto, no es tan solo un ámbito clave para llevar a cabo operaciones sino que también es un ámbito *habilitador* clave para llevar a cabo operaciones dentro de los ámbitos físicos. Como tal, el DOD es responsable de la seguridad y protección de su propia infraestructura en el espacio cibernético. Sin embargo, de ser necesario puede tomar "acción para disuadir o defender en contra de ataques cibernéticos que constituyen una amenaza inminente para la seguridad nacional".[35] Con respecto a esta responsabilidad, al igual que las funciones acompañantes del DHS, "en circunstancias extraordinarias, el Presidente, en calidad de Comandante en Jefe, o el Congreso, pueden autorizar acciones militares para contrarrestar las amenazas a Estados Unidos. Por lo tanto, el DOD puede llevar a cabo misiones como el principal en defender a Estados Unidos. En dichas circunstancias, el DHS, a través del NCCIC, lleva a cabo sus procesos y con sus socios para apoyar las misiones del DOD".[36] Al hacer esto, el DOD garantiza la seguridad de sus redes e infraestructura del espacio cibernético y, cuando el Presidente o el Congreso lo autorizan, lleva a cabo actividades en el espacio cibernético para defender a Estados Unidos y sus intereses nacionales.

Dentro del DOD, el secretario de defensa encomendó "las responsabilidades de la misión ciberespacial al Comando Estratégico de Estados Unidos (USSTRATCOM, por sus siglas en inglés), a otros Comandos Combatientes y a los Departamentos Militares".[37] El USCYBERCOM, actualmente un comando subunificado bajo el USSTRATCOM, "planifica, coordina, integra, sincroniza y lleva a cabo actividades para: dirigir las operaciones y la defensa de redes de informáticas específicas del Departamento de Defensa y prepararse para y, cuando se le ordena, llevar a cabo el espectro total de operaciones militares en el espacio cibernético para poder permitir acciones en todos los ámbitos, garantizar libertad de acción en el espacio cibernético entre EUA y los Aliados y negarle lo mismo a nuestros adversarios".[38] Claramente, para el DOD, el USSTRATCOM tiene las responsabilidades de funcionar en el espacio cibernético, pero la mayoría de las capacidades ciberespaciales del departamento radican dentro del comando subordinado, el USCYBERCOM.

Otro comando combatiente en el DOD con un interés en la defensa y seguridad del espacio cibernético, el USNORTHCOM, planifica, organiza y ejecuta las misiones de defensa. Específicamente, "defiende el suelo patrio estadounidense —protegiendo a nuestro pueblo, poder nacional y libertad de acción".[39] Con respecto al espacio cibernético, USNORTHCOM no tiene una misión específicamente definida, sin embargo, ningún ámbito definido se asocia con la defensa nacional. Por lo tanto, las misiones definidas en la actualidad parecen requerir que el comando defienda la patria en el ámbito del espacio cibernético junto con los ámbitos físicos.

El director de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), una agencia que también está involucrada en el espacio cibernético, tiene dos responsabilidades (o sea, desempeña dos puestos simultáneamente) en calidad de comandante del CYBERCOM. La NSA "está al frente del gobierno de EUA en criptología que abarca la inteligencia de señales (SIGINT, por sus siglas en inglés) y los productos y servicios de la seguridad de la información (IA, por sus siglas en inglés) y habilita las Operaciones en la Red de Computadoras (CON, por sus siglas en inglés) para poder lograr una ventaja decisiva para la nación y nuestros aliados bajo todas circunstancias".[40] Aunque su director está en el DOD, las misiones y responsabilidades de la NSA van más allá de un departamento, proporcionando "productos y servicios al Departamento de Defensa, la comunidad de inteligencia, a las agencias gubernamentales, socios en la industria y a aliados elegidos y socios de la coalición".[41] El conocimiento de la información de la NSA le proporciona al comandante del USCYBERCOM un mejor entendimiento del entorno del espacio cibernético.

Recomendaciones

Cualquier detalle del entorno ciberespacial y sus funciones, responsabilidades y autoridades del sector privado y de las agencias gubernamentales estadounidenses naturalmente suscitan dos preguntas. ¿Son capaces de llevar a cabo esas tareas las agencias encargadas con ciertas funciones y responsabilidades? ¿Son adecuadas las autoridades otorgadas a las agencias responsables para permitirles que aseguren y defiendan el espacio cibernético según se requiera? Sostenemos que la respuesta a ambas preguntas es no. Según la Revisión del 2011 de la *Política del Espacio Cibernético* creada por la Oficina del Presidente de Estados Unidos, el gobierno estadounidense "no está organizado para tratar eficazmente el problema del espacio cibernético ni ahora ni en el futuro. Las responsabilidades por la seguridad cibernética están distribuidas a lo largo de una amplia gama de departamentos y agencias federales, muchas con autoridades que se superponen entre sí, y ninguna con suficiente autoridad de decisión para dirigir de manera consistente acciones que tienen que ver con cuestiones que a menudo son conflictivas".[42] Si se supone que Estados Unidos deba adecuadamente "defender sus redes, ya sea que la amenaza proviene de terroristas, delincuentes cibernéticos o estados y sus representantes", entonces las funciones, responsabilidades y autoridades dentro del espacio cibernético de las agencias gubernamentales necesitan alterarse.[43]

El primer cambio importante tiene que ver con el DIB al igual que los propietarios y operadores CIKR dentro del sector privado. Las compañías y corporaciones que componen el DIB y apoyan al DOD deben incorporar medidas de seguridad cibernética que cumplan con las normas del DOD. Esta iniciativa indudablemente enfrentará resistencia; muchas alegarán que consiste en una invasión de la privacidad o que el "gran hermano" las está vigilando. Además, alterar las normas y protocolos de seguridad involucra costes intrínsecos (en términos de dólares, tiempo, recursos, etc.). El mejor método para evitar esas inquietudes exige requerir este nivel de seguridad cibernética como parte de adjudicar cualesquier contratos nuevos del DOD y actualizar los existentes. Además, todos los contratos nuevos o actualizados deben incluir informar cualesquier intrusiones, ataques o violaciones ciberespaciales. Para facilitar los informes, las compañías y corporaciones DIB deben acatar las normas de seguridad cibernética establecidos por el NIST y conectarse al NCCIC, quien a su vez comparte información relevante con las agencias apropiadas (Fuerza de Tarea Conjunta Nacional de Investigaciones Cibernéticas, USCYBERCOM, USNORTHCOM, etc.).

Las leyes actuales excluyen al gobierno de EUA de imponer requisitos contractuales a propietarios y operadores del CIKR. No obstante, el NIST estableció un marco de seguridad cibernética "para comprender, administrar y expresar los riesgos a la seguridad cibernética".[44] La mayoría de los servicios y productos provistos por los propietarios y operadores del CIKR son esenciales para los ciudadanos estadounidenses pero no son financiados contractualmente por el gobierno estadounidense; por lo tanto, éste último no puede exigir acuerdos contractuales similares a aquellos con las compañías y corporaciones DIB. Un método apropiado para cerciorarnos que muchos propietarios y operadores CIKR acatan las mismas condiciones impuestas en el DIB y las normas establecidas por el NIST tiene que ver con la inclusión de términos contractuales en cualquier seguro, subsidios, subvenciones y así sucesivamente que reciban provistos por el gobierno estadounidense. Para poder calificar para recibir fondos provistos por el gobierno, los propietarios y operadores CIKR deben establecer un requisito previo para la seguridad cibernética al igual que una garantía de reportar a la NCCIC cualesquier intrusiones, ataques o violaciones al espacio cibernético. Una medida adicional para persuadirlos a que participen voluntariamente tiene que ver con proveerles (sin costo alguno) con el software de seguridad cibernética y garantía de la información del DOD y ofrecerles el entrenamiento con la estipulación de que cualesquier intrusiones, ataques o violaciones se deben notificar a la NCCIC. Lamentablemente,

no hay ninguna panacea para la seguridad cibernética dentro del sector privado. Sin embargo, al modificar algunos requisitos, el gobierno estadounidense mejora la seguridad dentro del DIB, al igual que los propietarios y operadores CIKR, y realza los requisitos para reportar los incidentes de seguridad cibernética.

Con respecto a las agencias del gobierno de EUA, el presidente o el secretario de defensa imponen las demandas o restricciones deseadas. El primer paso importante en mejorar la seguridad cibernética y la defensa de EUA es activar al USCYBERCOM con un comando combatiente completamente funcional en lugar de un comando subunificado bajo el USSTRATCOM. Aunque en la actualidad no hay una fecha de activación específica, la preparación comenzó hace varios años. Las amenazas y ataques cibernéticos actuales exigen que esta acción se complete tan pronto sea posible. En calidad de la agencia con el mejor entendimiento de las amenazas cibernéticas, el USCYBERCOM debe ser designado nuevamente como la agencia principal para crear e implementar las medidas de seguridad cibernética a lo largo de los las agencias gubernamentales estadounidenses (por autoridad del Título 40 del Código de EUA) y de los propietarios/operadores DIB y CIKR discutidos anteriormente (por autoridad de los Títulos 10 y 32, respectivamente, del Código de EUA). Lamentablemente, este paso exigirá reducciones simultáneas en las responsabilidades del DHS, que se explican a continuación. El USCYBERCOM también debe trabajar con los servicios armados para crear capacidades y entrenamiento para el personal que detecta y responde a los ataques en el ámbito cibernético (si el presidente, o el secretario de defensa, deben autorizar la respuesta). De hecho, el USCYBERCOM está anticipando un flujo de personal masivo de 900 personas entre el 2014 y el 2016, se ha programado que los miembros del servicio activo llenarán el 80% de esos puestos y el resto serán civiles.[45] Además, el USCYBERCOM "activó el cuartel general para su *Cyber National Mission Force* (Fuerza Cibernética para la Misión Nacional) para reaccionar ante ataques cibernéticos a la nación".[46] Lamentablemente, establecer un nuevo comando combatiente que se concentre principalmente en ámbitos específicos genera otros retos. Por ejemplo, el entorno fiscal austero impone restricciones en las finanzas de los servicios militares, tornando difícil de justificar los gastos de fondos en un problema subestimado y difícil de definir.

La función de la NSA en la seguridad cibernética también necesita modificación. Su capacidad para determinar las indicaciones y las advertencias de un ataque inminente o en curso —al igual que atribuir ataques a actores individuales, grupos o naciones estados— necesita más utilización por el gobierno de EUA en la seguridad cibernética. La NSA debe tener conexión con la NCCIC para facilitar el intercambio de inteligencia y de información a lo largo del ámbito cibernético. Además, en vista de que el director de la agencia es también el comandante del USCYBERCOM, las dos entidades pueden crear conjuntamente las normas y medidas de seguridad mencionadas anteriormente y por ende dar lugar a un mejor producto. Lamentablemente, esta función doble de un solo comandante con autoridades a ambos Título 10 y Título 50 del Código de EUA, continúa siendo una propuesta tenue para muchos miembros del Congreso. La rectificación de esta polémica es esencial si es que se crea un comando combatiente unificado.

Aunque el USNORTHCOM es el comando combatiente encomendado específicamente con la defensa nacional, una asociación entre el mismo y el USCYBERCOM para la defensa en el ámbito cibernético se debe codificar. Hay una asociación similar entre el USNORTHCOM y el USSTRATCOM en el entorno espacial. El USCYBERCOM retiene las capacidades y debe contar con las autoridades para la seguridad cibernética y la defensa, pero no puede determinar si un ataque cibernético es un precursor a o una porción a un ataque más grande. Para remediar esta deficiencia, el USNORTHCOM requiere integración completa a la NCCIC para garantizar la disponibilidad de una descripción detallada del entorno de la defensa nacional a lo largo de todos los ámbitos —aire, tierra, mar, espacio (con el USSTRATCOM) y el espacio cibernético. Entender las amenazas en todos los ámbitos le permite al comandante del USNORTHCOM pro-

veerle al presidente o al secretario de defensa una evaluación de ataques actuales o esperados en contra de la nación.

La función del DHS también exige que se defina nuevamente. Aunque en la actualidad es la agencia principal para la seguridad cibernética, el departamento no puede llevar a cabo esta función. Aunque el DHS debe retener la responsabilidad de asegurar la infraestructura crítica en el ámbito físico, el presidente debe redefinir su función de la seguridad cibernética para incluir la coordinación de la inteligencia en la seguridad cibernética y la porción de la gestión de consecuencias para efectos después de un ataque cibernético que resulte en daños físicos. Para la respuesta de gestión en casos de crisis, la Agencia Federal para la Gestión de Emergencias (FEMA, por sus siglas en inglés) del DHS continúa siendo la organización principal. La NCCIC del DHS debe continuar funcionando en su capacidad actual; sin embargo, el USCYBERCOM debe contar con la propiedad compartida o supervisión compartida de este centro. En vista de que el USCYBERCOM conserva más capacidades de seguridad cibernética y de defensa cibernética, su participación adicional realza las capacidades de la NCCIC. Además esta supervisión doble por parte del DHS (bajo la autoridad del Título 6 del Código de EUA) y del DOD (bajo la autoridad del Título 10 del Código de EUA) evita la dependencia en una sola agencia para la seguridad cibernética. Por último, la participación cada vez mayor del USCYBERCOM en la NCCIC mejora el conocimiento de la situación del DOD dentro del ámbito ciberespacial.

El DOJ debe conservar su enfoque en el terrorismo cibernético e implementar solamente alteraciones pequeñas en sus funciones y responsabilidades. El FBI debe continuar como la agencia principal que opera internamente para proteger y defender el ámbito cibernético contra ataques terroristas al igual que mantener la Fuerza de Tarea Conjunta Nacional de Investigaciones Cibernéticas. Sin embargo el USCYBERCOM, debe tener la responsabilidad de defender contra amenazas cibernéticas que emanan de agencias de inteligencia extranjeras auspiciadas por los estados. Los ataques e intrusiones de esos actores requieren el análisis apropiado para definir si son parte de un ataque mayor en el territorio estadounidense. Observen que ninguno de estos cambios propuestos ni afectan ni cambian las autoridades de investigación ni las funciones del FBI, que debe continuar siendo la agencia federal principal para llevar a cabo las actividades de cumplimiento de la ley.

Conclusión

El futuro de la seguridad cibernética, la defensa cibernética y la respuesta cibernética de Estados Unidos no está claro. Sin embargo, las políticas que en la actualidad definen las autoridades, funciones y responsabilidades no tratan adecuadamente la amenaza cada vez mayor en el ámbito del espacio cibernético. Con algunos cambios dramáticos dentro de las autoridades y responsabilidades, el gobierno de Estados Unidos podría mejorar drásticamente su capacidad para proteger a los ciudadanos estadounidenses de las amenazas cibernéticas. Específicamente, las compañías y corporaciones que comprenden el DIB y que apoyan al DOD deben incorporar medidas de seguridad cibernética que cumplan con las normas del DOD. El USCYBERCOM debe ser designado un comando combatiente funcional, debe compartir el control y supervisión de la NCCIC con el DHS y debe ser encomendado con las responsabilidades en los ámbitos de la seguridad cibernética, defensa cibernética y respuesta cibernética bajo la autoridad de los Títulos 10 y 32 del Código de EUA. El USNORTHCOM requiere integración con el USCYBERCOM a través de la NCCIC; como un comando combatiente encargado de la defensa nacional, el USNORTHCOM debe analizar una gama más amplia de amenazas (a lo largo de los entornos físicos y virtuales) para determinar si un ataque cibernético es parte de un ataque mayor en general por parte de una nación estado. El DHS debe conservar la responsabilidad de asegurar la infraestructura crítica en el ámbito físico. La función de seguridad cibernética del DHS debe ser reducida de manera que incluya solamente la porción de gestión de consecuencias (por la Agencia Fede-

ral para la Gestión de Emergencias) para efectos después de un ataque cibernético que resulte en daños físicos. La incorporación de estas recomendaciones realzará la mitigación de estos tipos de retos e inquietudes. ❑

Notas

1. Oficina del Presidente de Estados Unidos, Cyberspace Policy Review (Revisión de la política ciberespacial) (Washington, DC: Casa Blanca, 2011), i, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
2. Oficina del Presidente de Estados Unidos, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Estrategia internacional para el espacio cibernético: Prosperidad, seguridad y franqueza en un mundo interconectado) (Washington, DC: Casa Blanca, mayo de 2011), 12, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
3. Oficina del Presidente de Estados Unidos, Cyberspace Policy Review, iii.
4. Departmento de Defensa, Department of Defense Strategy for Operating in Cyberspace (Estrategia del Departamento de Defensa para operar en el espacio cibernético) (Washington, DC: Department of Defense, julio de 2011), 5, http://www.defense.gov/news/d20110714cyber.pdf.
5. Oficina del Presidente de Estados Unidos, National Security Strategy (Estrategia de seguridad nacional) (Washington, DC: Casa Blanca, mayo de 2010), 27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
6. Departamento de Defensa, Strategy for Operating in Cyberspace, 3.
7. Ibid., 4.
8. Oficina del Secretario de Prensa, "Presidential Policy Directive/PPD-21" (Directriz presidencial / PPD-21) (Washington, DC: Office of the Press Secretary, White House, 12 de febrero de 2013), 5, https://fas.org/irp/offdocs/ppd/ppd-21.pdf.
9. Departamento de Defensa, Strategy for Operating in Cyberspace, 8.
10. Oficina del Subsecretario de Defensa de Estados Unidos, a los líderes del Departamento de Defensa, memorando, asunto: Seguridad cibernética de la base industrial de la defensa, octubre de 2012, párrafo 1.
11. Ibid., párrafo 3.
12. Ibid.
13. Departamento de Seguridad Nacional, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency (Plan de protección para la infraestructura nacional: Asociándose para realzar la protección y la resistencia) (Washington, DC: Department of Homeland Security, 2009), 109, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
14. Ibid., 110.
15. Departamento de Seguridad Nacional, National Cyber Incident Response Plan (Plan de respuesta nacional en caso de un incidente cibernético), versión interina (Washington, DC: Department of Homeland Security, septiembre de 2010), 7–8, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.
16. Oficina del Secretario de Prensa, Executive Order —Improving Critical Infrastructure Cybersecurity (Orden ejecutiva— mejorando la seguridad cibernética de la infraestructura crítica), (Washington, DC: White House, 12 de febrero de 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
17. Ibid.
18. Oficina del Presidente de Estados Unidos, "Homeland Security Presidential Directive-7" (Directriz presidencial 7 de seguridad nacional) (Washington, DC: White House, diciembre de 2003), párrafo 16, https://www.dhs.gov/homeland-security-presidential-directive-7.
19. Departamento de Seguridad Nacional, National Cyber Incident Response Plan, 5.
20. Ibid., 24n43.
21. Oficina del Secretario de Prensa, "Presidential Policy Directive/PPD-21," [3].
22. Eric A. Fischer, Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, (Leyes federales relacionadas con la seguridad cibernética: Reseña y discusión de revisiones propuestas), Informe CRS para el Congreso R42114 (Washington, DC: Congressional Research Service, 20 de junio de 2013), 9, http://www.fas.org/sgp/crs/natsec/R42114.pdf.
23. "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments" (NIST disemina marco de seguridad cibernética preliminar, buscará comentarios) National Institute of Standards and Technology, 22 de octubre de 2013, http://www.nist.gov/itl/cybersecurity-102213.cfm.
24. Amber Corrin, "DHS Feels Growing Pains in Cybersecurity Role" (DHS siente dificultades en su función de seguridad cibernética), FCW, 17 de octubre de 2012, http://fcw.com/articles/2012/10/17/dhs-cybersecurity.aspx.
25. Oficina del Presidente de Estados Unidos, "Homeland Security Presidential Directive-7," párrafo 22 (a).

26. Departamento de Seguridad Nacional, National Cyber Incident Response Plan, 6.
27. Ibid.
28. Oficina del Secretario de Prensa, "Presidential Policy Directive/PPD-21," [4].
29. "National Cyber Investigative Joint Task Force" (Fuerza Nacional de Tarea Conjunta de Investigación Cibernética) Federal Bureau of Investigation (Buró Federal de Investigaciones), consultado el 9 de marzo de 2013, http://www.fbi.gov/about-us/investigate/cyber/ncijtf. Consultar también Oficina del Secretario de Prensa, "Presidential Policy Directive/PPD-21," [4].
30. "Cybersecurity" (Seguridad cibernética) Departamento de Energía, consultado el 6 de marzo de 2014, http://energy.gov/oe/services/cybersecurity.
31. Instituto Nacional de Estándares y Tecnología, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements (Pautas para seguridad cibernética en redes eléctricas: Vol 1, Estrategia, arquitectura y requerimientos de alto nivel para seguridad cibernética en redes eléctricas) (Washington, DC: National Institute of Standards and Technology, agosto de 2010), 1, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.
32. "Cybersecurity," Departamento de Energía.
33. Departamento de Defensa, Strategy for Operating in Cyberspace, 1.
34. Departamento de Defensa, Quadrennial Defense Review Report (Informe cuadrienal de revisión de la defensa) (Washington, DC: Department of Defense, febrero de 2010), 37, http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf.
35. Departamento de Seguridad Nacional, National Cyber Incident Response Plan, C-2.
36. Ibid., 10.
37. Departamento de Defensa, Strategy for Operating in Cyberspace, 5.
38. "US Cyber Command Factsheet" (Hoja informativa del Comando Cibernético de EUA), Comando Estratégico de EE.UU., consultado el 5 de septiembre de 2014, http://www.stratcom.mil/factsheets/2/Cyber_Command/.
39. "About USNORTHCOM" (Acerca del USNORTHCOM), Comando Norte de EUA, consultado el 5 de septiembre de 2014, http://www.northcom.mil/aboutUSNORTHCOM.aspx.
40. "About NSA" (Acerca de la NSA), Agencia de Seguridad Nacional, consultado el 13 de febrero de 2013, https://www.nsa.gov/about/mission/index.shtml.
41. Ibid.
42. Oficina del Presidente de Estados Unidos, Cyberspace Policy Review, i.
43. Oficina del Presidente de Estados Unidos, International Strategy for Cyberspace (Estrategia Internacional para el Espacio Cibernético), 12.
44. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, versión 1.0 (Washington, DC: National Institute of Standards and Technology, 12 de febrero de 2014), 7, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
45. Andrew Tilghman, "Cyber Command to Hire Thousands Of Troops, Civilians" (Comando Cibernético empleará a miles de tropas y civiles), DefenseNews, 12 de febrero de 2013, http://www.defensenews.com/article/20130212/C4ISR01/302120026/Cyber-Command-Hire-Thousands-Troops-Civilians.
46. Cheryl Pellerin, "Cybercom Activates National Mission Force Headquarters" (Comando Cibernético activa Cuartel General de Fuerza de Misión Nacional) Departamento de Defensa de EUA, 25 de septiembre de 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854.

Teniente Coronel August G. Roesener, PhD, USAF (USAFA; MS, University of Florida; PhD, University of Texas; MMOAS [Master of Military Operational Art and Science], Air University), en la actualidad se desempeña como el analista principal para el Cuartel General, Comando de Movilidad Aérea, Base Aérea Scott, Illinois. Anteriormente llevó a cabo evaluaciones de planes de campaña en calidad de analista aéreo conjunto en el Comando Norteamericano de Defensa Aeroespacial, Comando del Norte de EUA, Base Aérea Peterson, Colorado.

Mayor Carl Bottolfson, USAF (BA, University of Wisconsin; MA, Trident University International) se desempeña en calidad de jefe de política en la plana del Agente Ejecutivo para el Espacio en el Departamento de Defensa. Recibió su comisión a través del ROTC en la Universidad de Wisconsin en el 2000. Antes de desempeñar su puesto actual, el Mayor Bottolfson se desempeñó en calidad de jefe de política espacial en el Comando Estratégico de Estados Unidos y jefe de operaciones de conocimiento de la situación en el Centro Conjunto de Operaciones Espaciales, Base Aérea Vandenberg, California.

Capitán de Fragata Gerry Fernández, USN (BS, San Diego State University; MS, Naval Postgraduate School) se desempeña como jefe de sección en gestión a nivel de servicio y requerimientos de los sistemas de informática en el Cuartel General de la Organización del Tratado del Atlántico Norte (OTAN), Comandante Supremo Aliado de Transformación. Recibió su comisión a través del ROTC en San Diego State University en 1992. El Capitán de Fragata Fernández trabajó en la plana del comandante, Fuerza de Tarea Conjunta Cono de África, en Djibouti, África.