Defendiendo un Nuevo Ámbito

La Ciberestrategia del Pentágono*

William J. Lynn III, Secretario Adjunto de Defensa de EE.UU.

EN ESTE MOMENTO, más de cien organizaciones extranjeras de inteligencia están tratando de lograr el acceso a las redes digitales que aseguran las operaciones militares de Estados Unidos. El Pentágono reconoce la amenaza catastrófica que la ciberguerra representa y se está asociando con gobiernos aliados y empresas privadas para prepararse.

En el 2008, las redes clasificadas de las computadoras militares del Departamento de Defensa se vieron significativamente comprometidas. Comenzó cuando una unidad *flash* infectada fue introducida en una computadora portátil (*laptop*) en una base en el Oriente Medio.

El código de computadora malicioso de la unidad *flash,* colocada ahí por una agencia de inteligencia extranjera, se autocargó a una red administrada por el Comando Central de Estados Unidos. Ese código se esparció sin ser detectado en los sistemas clasificados y no clasificados, estableciendo lo que equivale a un puesto de avanzada digital, del cual se podían transferir datos a servidores bajo control extranjero.

Fue el peor temor de un administrador de red: un programa paria funcionando silenciosamente, listo para entregar planes operacionales en las manos de un adversario desconocido.

Este incidente fue la infracción más significativa a las computadoras militares de Estados Unidos y sirvió como una alerta importante. La operación del Pentágono para contrarrestar el ataque, conocida como Operación Buckshot Yankee, marcó un momento decisivo para la estrategia de ciberdefensa de Estados Unidos.

Durante los últimos diez años, la frecuencia y complejidad de las intrusiones a las redes militares estadounidenses han aumentado exponencialmente. Todos los días, las redes militares y civiles de Estados Unidos son sondeadas miles de veces y escaneadas millones de veces.

Y la intrusión en el 2008 que culminó en la Operación Buckshot Yankee no fue la única penetración exitosa. Los adversarios han adquirido miles de archivos de las redes estadounidenses y de las redes de aliados de Estados Unidos y socios en la industria, inclusive copias de planos de armamento, planes operacionales y datos de vigilancia.

A medida que ha aparecido la escala de la amenaza de la ciberguerra a la seguridad nacional y a la economía de Estados Unidos, el Pentágono ha creado defensas en etapas y robustas alrededor de las redes militares e inauguró el nuevo Comando Cibernético de Estados Unidos para integrar operaciones de ciberdefensa en la milicia.

El Pentágono está colaborando con el Departamento de Seguridad Nacional para proteger las redes del gobierno y la infraestructura crítica, y con los aliados más allegados de Estados Unidos para extender internacionalmente esas defensas. Aún queda por hacer una enorme cantidad de trabajo básico, pero el gobierno de Estados Unidos ha comenzado a establecer varias iniciativas para defender al país en la era digital.

---

*Fuente: Publicado con permiso de *Foreign Affairs Magazine*, Septiembre/Octubre 2010.

ENTORNO DE LA AMENAZA

La tecnología de la informática es lo que permite casi todo lo que la milicia estadounidense realiza: apoyo logístico y mando y control global de las fuerzas, suministro de inteligencia en tiempo real y operaciones a distancia. Cada una de esas funciones depende en gran medida del eje de las comunicaciones globales de la milicia, que consta de 15,000 redes y siete millones de dispositivos de informática a lo largo de cientos de instalaciones en docenas de países. Más de noventa mil personas trabajan tiempo completo para darles mantenimiento. En menos de una generación, la tecnología de la informática en la milicia ha evolucionado de una herramienta administrativa para realzar la productividad en la oficina a un recurso estratégico nacional por derecho propio. La infraestructura digital del gobierno de Estados Unidos ahora le ofrece a la nación ventajas críticas sobre cualquier adversario, pero su dependencia en las redes de computadoras también potencialmente le permite a los adversarios obtener información valiosa de inteligencia sobre las capacidades y operaciones de Estados Unidos, para obstruir las fuerzas militares convencionales y perturbar el desarrollo de la economía de Estados Unidos. Al crear una estrategia para contrarrestar estos peligros, el Pentágono se está enfocando en unos cuantos atributos fundamentales de la ciberamenaza.

Primero, la ciberguerra es asimétrica. El bajo costo de los dispositivos de informática significa que los adversarios de EE.UU. no tienen que fabricar armamento costoso, tales como los aviones de combate furtivos o portaaviones, para representar una amenaza significativa a las capacidades de la milicia estadounidense. Una docena de programadores de computadoras determinados pueden, si encuentran una vulnerabilidad de la que aprovecharse, amenazar la red logística global de Estados Unidos, robar sus planes operacionales, cegar sus capacidades de inteligencia o socavar su capacidad de lanzar bombas en los blancos. Conociendo esto, muchos militares están creando capacidades de ofensiva en el ciberespacio, y más de cien organizaciones de inteligencia extranjeras están intentando irrumpir las redes estadounidenses. Algunos gobiernos ya cuentan con la capacidad de interrumpir elementos de la infraestructura de informática de Estados Unidos.

En el ciberespacio, la ofensiva lleva la delantera. La *Internet* fue concebida para ser colaborativa y se extendiera rápidamente y que tuviese barreras bajas a la innovación tecnológica; la gestión de la seguridad y la identidad eran prioridades bajas. Por esos motivos estructurales, la capacidad del gobierno de EE.UU. de defender sus redes siempre queda rezagada ante la capacidad del adversario de sacarle provecho a los puntos débiles de las redes estadounidenses. Los programadores expertos encontrarán vulnerabilidades y superan las medidas de seguridad establecidas para evitar las intrusiones. En un entorno donde domina la ofensiva, una mentalidad de fortaleza no funcionará. Estados Unidos no puede retirarse detrás de una Línea Maginot de *firewalls* o corre el riesgo de ser invadido. La ciberguerra es como la guerra de maniobras en la que la velocidad y la agilidad son de suma importancia. Para llevarle la ventaja a los que lo persiguen, Estados Unidos tiene que ajustar y mejorar constantemente sus defensas.

Además debe reconocer que los modelos tradicionales de disuasión de la Guerra Fría de represalia garantizada no aplican al ciberespacio, donde resulta difícil y toma mucho tiempo identificar el autor de un ataque. Mientras que un misil viene con un remitente, un virus de computadora por lo general no. La labor forense necesaria para identificar al agresor puede tomar meses, si es que la identificación fuese del todo posible. E inclusive cuando se identifica al agresor, si es un actor no estatal, como un grupo terrorista, puede que no cuente con recursos contra los cuales Estados Unidos puede tomar represalias. Además, no siempre está claro en qué consiste un ataque. De hecho, muchas de las intrusiones de hoy están más cerca al espionaje que a los actos de guerra. La ecuación de la disuasión se confunde aún más por el hecho de que los ciberataques a menudo originan de servidores infiltrados en países neutrales y que respuestas a ellos podrían tener consecuencias imprevistas.

En vista de las circunstancias, la disuasión necesariamente se basará más en negar cualquier beneficio a los agresores que en imponer costos a través de la represalia. El reto es lograr que las defensas sean lo suficientemente eficaces para negarle a un adversario el beneficio de un ataque a pesar de la fortaleza de las herramientas de ofensiva en el ciberespacio. (Regímenes tradicionales de control de armas probablemente fracasarían en disuadir ciberataques a causa de los retos de atribución, que hacen que la verificación del cumplimiento sea prácticamente imposible. Sí debe haber normas internacionales de comportamiento en el ciberespacio, ellas tienen que regirse por un modelo diferente, tales como el de salud pública o cumplimiento de la ley).

Las ciberamenazas a la seguridad nacional de EE.UU. no se limitan a blancos militares. Los *hackers* y los gobiernos extranjeros pueden lanzar cada vez más intrusiones a las redes que controlan la infraestructura civil crítica. Fallas inducidas por computadora a las redes de energía de EE.UU., a las redes de transporte o a los sistemas financieros podrían causar daños físicos masivos y trastornos económicos. Tal infraestructura es también esencial para la milicia, tanto en el extranjero como en el país: coordinar el despliegue y el reabastecimiento de tropas estadounidenses y dotar las tropas con productos de vendedores privados necesariamente exige que se empleen redes no clasificadas que están unidas a la *Internet* abierta. Proteger esas redes y las redes que apoyan a la infraestructura crítica de Estados Unidos tiene que ser parte de las misiones de seguridad nacional y de defensa nacional de Washington.

La tecnología moderna de la informática también aumenta el riesgo del espionaje industrial y el robo de información comercial. A inicios de este año, Google reveló que había perdido su propiedad intelectual como resultado de una operación compleja perpetrada contra su infraestructura corporativa, una operación que también atacó docenas de otras compañías. Aunque la amenaza a la propiedad intelectual es menos dramática que la amenaza a la infraestructura nacional crítica, puede que sea la ciberamenaza más significativa que Estados Unidos enfrentará a largo plazo. Anualmente, una cantidad de propiedad intelectual mucho más grande que toda la propiedad intelectual contenida en la Biblioteca del Congreso es robada de redes mantenidas por negocios, universidades y agencias gubernamentales estadounidenses. En vista de que la fortaleza militar en un final depende de la vitalidad económica, pérdidas constantes de la propiedad intelectual podrían desgastar tanto la eficacia de la milicia estadounidense como su competitividad en la economía global.

Las redes de computadoras en sí no son la única vulnerabilidad. El *software* y el *hardware* están en riesgo de ser alterados inclusive antes de que estén enlazados juntos en un sistema operacional. Un código paria, inclusive las conocidas bombas lógicas que causan fallas inesperadas, puede ser introducido en el *software* cuando se está diseñando. En cuanto al *hardware*, "interruptores cortacorriente" (*kills switches*) operados por control remoto y "puertas traseras" (*backdoors*) escondidas se pueden escribir en los chip de las computadoras que usan los militares, permitiendo que actores externos puedan manipular los sistemas de lejos. El riesgo de comprometer el proceso de fabricación es muy real y quizás sea la ciberamenaza menos entendida. La interferencia es prácticamente imposible de detectar e inclusive más difícil de erradicar. Ya se ha detectado *hardware* de contrabando en sistemas que el Departamento de Defensa ha comprado. El *Trusted Foundries Program* del Pentágono, que certifica las piezas creadas por fabricantes de microelectrónica, es un buen comienzo, pero no es una solución exhaustiva a los riesgos de la base tecnológica del Departamento de Defensa. *Microsoft* y otras compañías de tecnología de computadoras han diseñado estrategias complejas para la mitigación de riesgos con el fin de detectar códigos maliciosos y disuadir su inclusión en sus cadenas de abastecimiento global; el gobierno de Estados Unidos necesita emprender una iniciativa similar para las aplicaciones críticas civiles y militares.

Estados Unidos rara vez predice con precisión cuándo y dónde los conflictos tendrán lugar. Predecir ciberataques también se está tornando difícil, especialmente ya que tanto los

actores estatales como los no estatales representa amenazas. Más importante aún, en vista de que la tecnología de la informática está evolucionando rápidamente, los encargados de formular la política se quedan con pocos precedentes históricos para informar sus expectativas. Por lo tanto, el gobierno estadounidense debe ser modesto acerca de su capacidad para saber cuándo y cómo esta amenaza podría madurar; lo que necesita es una estrategia que ofrezca flexibilidad operacional y capacidades que ofrezcan una máxima adaptabilidad.

ESTRATEGIA NUEVA

Como una cuestión de doctrina, el Pentágono ha reconocido oficialmente al ciberespacio como el nuevo ámbito de la guerra. Aunque el ciberespacio es un ámbito hecho por el hombre, se ha tornado igual de crítico para las operaciones militares como lo son la tierra, el mar, el aire y el espacio. Como tal, la milicia debe poder defender y operar dentro de él. Para facilitar las operaciones en el ciberespacio, el Departamento de Defensa necesita una estructura organizativa apropiada. Durante los últimos años, la iniciativa de ciberdefensa de la milicia estaba dirigida por una confederación libre de fuerzas de tareas conjuntas dispersadas tanto geográfica como institucionalmente. En junio de 2009, reconociendo que la escala de esfuerzo para proteger el ciberespacio había superado las estructuras existentes de la milicia, el Secretario de Defensa, Robert Gates, ordenó la consolidación de las fuerzas de tarea en un solo comando con un general de cuatro estrellas al frente, el Comando Cibernético de Estados Unidos, el cual comenzó las operaciones en mayo de 2010 como parte del Comando Estratégico de Estados Unidos. Se proyecta que el Comando Cibernético estará completamente operacional para octubre.

El Comando Cibernético tiene tres misiones. Primero, está al frente de la protección diaria de todas las redes de defensa y apoya las misiones militares y contraterroristas con operaciones en el ciberespacio. Segundo, provee una manera clara y responsable de ordenar los recursos de la ciberguerra de toda la milicia. Una sola cadena de mando va desde el presidente de Estados Unidos al secretario de defensa, al comandante del Comando Estratégico al comandante del Comando Cibernético y de ahí a las unidades militares individuales alrededor del mundo. Para garantizar que las consideraciones de ciberseguridad sean parte regular del adiestramiento y equipamiento de los soldados, el Comando Cibernético supervisa los comandos dentro de cada servicio armado de la milicia, inclusive el Comando Cibernético de las Fuerzas del Ejército, la Décima Flota de la Armada de Estados Unidos, la Vigésima Cuarta Fuerza Aérea y el Comando Ciberespacial de las Fuerzas del Cuerpo de Infantería de Marina. En vista de que las redes militares no son insensibles al ataque, una parte crítica de la misión de entrenamiento es garantizar que todas las fuerzas operacionales puedan funcionar en un entorno de información degradado.

La tercera misión del Comando Cibernético es trabajar con una variedad de socios dentro y fuera del gobierno de Estados Unidos. Representantes del FBI, del Departamento de Seguridad Nacional, del Departamento de Justicia y de la Agencia de Sistemas de Informática de la Defensa trabajan en el cuartel general del Comando Cibernético, en el Fuerte Meade, al igual que oficiales de enlace de la comunidad de inteligencia y de gobiernos aliados. En colaboración con el Departamento de Seguridad Nacional, el Comando Cibernético también trabaja muy de cerca con la industria privada para compartir información acerca de amenazas y para tratar vulnerabilidades compartidas. Las redes de informática conectan una variedad de instituciones, por lo tanto el esfuerzo para defender a Estados Unidos solamente tendrá éxito si se coordina con todo el gobierno, con los aliados y con los socios en el sector comercial.

En vista de la preponderancia de la ofensa en el ciberespacio, las defensas de Estados Unidos deben ser dinámicas. Milisegundos pueden hacer una diferencia, por lo tanto la milicia estadounidense debe responder a los ataques a medida que suceden o inclusive antes de que sucedan. Para lidiar con esto, el

Pentágono ha desplegado un sistema que incluye tres líneas de defensa que se traslapan. Dos se basan en las mejores prácticas comerciales—la higiene normal en las computadoras, que mantiene el *software* de seguridad y los *firewalls* actualizados, y los sensores que detectan y trazan las intrusiones. La tercera línea de protección le saca provecho a las capacidades de inteligencia del gobierno para proveer defensas activas sumamente especializadas. Y el gobierno está desplegando todas esas defensas de una manera que cumpla con su obligación de proteger las libertades civiles de los ciudadanos estadounidenses.

La Agencia de Seguridad Nacional ha sido la primera en aplicar sistemas que, empleando advertencias provistas por las capacidades de inteligencia de EE.UU., automáticamente despliega defensas para contrarrestar las intrusiones en tiempo real. Parte sensores, parte centinelas y parte francotiradores, esos sistemas de defensa activa representan un cambio fundamental en el método que EE.UU. emplea para la defensa de la red. Ellos trabajan colocando tecnología de barrido en el interfaz de las redes militares y la *Internet* abierta para detectar y detener códigos maliciosos antes de que se infiltren en las redes militares. Ahora, las defensas activas protegen todas las redes de defensa y de inteligencia en el ámbito ".mil".

En vista de que algunas intrusiones inevitablemente eludirán la detección y no se pueden atrapar en el límite, las ciberdefensas de Estados Unidos tienen que poder encontrar a los intrusos una vez que están adentro. Esto requiere poder cazar dentro de las propias redes de la milicia—una tarea que también es parte de la capacidad de defensa activa del Pentágono.

La defensa activa se ha hecho posible consolidando las capacidades colectivas de ciberdefensa del Departamento de Defensa bajo un solo techo y uniéndolas con la inteligencia de señales necesaria para prever intrusiones y ataques. Establecer este enlace fue uno de los motivos más importantes para crear el Comando Cibernético.

La velocidad a la cual los sistemas de defensa activa deben actuar significa que las reglas de enfrentamiento que rigen la defensa de la red deben establecerse en gran parte por adelantado. No es fácil concebir esos protocolos. De hecho, la iniciativa para definir reglas de enfrentamiento claras para responder a los ciberataques ha sido excesivamente difícil, y con razón aparente. Esas reglas de enfrentamiento primero tendrán que asistir en distinguir entre las hazañas de un simple *hacker*, actividad delictiva (tal como fraude y robo), espionaje y un ataque a los Estados Unidos. Luego tendrán que definir cuál acción es necesaria, correcta, proporcional y justificada en cada caso en particular con base en las leyes que rigen la acción en tiempos de guerra y de paz.

Los mejores planes para defender las redes militares tendrán poco valor si la infraestructura civil—que podría ser atacada directamente en un conflicto militar o convertirse en rehén y ser usada como moneda de cambio contra el gobierno de EE.UU. —no está segura. El Departamento de Defensa depende de la infraestructura de la tecnología de informática en general de Estados Unidos. Por ejemplo, depende de muchas redes externas en los ámbitos ".gov" y ".com", inclusive aquellas administradas por contratistas del Departamento de Defensa, que no están protegidas tan eficazmente como la propia red de los militares. El Departamento de Seguridad Nacional está a la vanguardia en la protección de los ámbitos ".gov" y ".com", pero el Pentágono debe sacarle provecho a sus diez años de inversión conjunta en la ciberdefensa para apoyar iniciativas más amplias para proteger la infraestructura crítica.

El gobierno de EE.UU. recién ha comenzado a abordar la pregunta más amplia de si es o no necesario y correcto utilizar recursos nacionales, tales como las defensas que ahora protegen a las redes militares, para proteger la infraestructura civil. Los encargados de formular las leyes deben tomar en cuenta, entre otras cosas, aplicar las capacidades de defensa de la Agencia de Seguridad Nacional más allá del ámbito ".gov", como por ejemplo a ámbitos que apoyan la industria de defensa comercial. Contratistas de la defensa de EE.UU. ya han sido señalados para la intrusión y sistemas de armamento delicados ya han sido compro-

metidos. Por lo tanto, el Pentágono está colaborando con el Departamento de Seguridad Nacional y el sector privado para encontrar maneras más innovadoras de emplear las capacidades de ciberdefensa de la milicia para proteger la industria de la defensa.

En vista de la naturaleza global de la *Internet*, los aliados de EE.UU. también desempeñan un papel crítico en la ciberdefensa. Mientras más firmas de un ataque uno pueda ver, y mientras más intrusiones uno pueda rastrear, mejores serán nuestras defensas. De esta manera, el modelo de advertencia compartida—una doctrina básica de la Guerra Fría—aplica al ciberespacio. Al igual que las defensas aérea y espacial de EE.UU. están enlazadas con las de los aliados para proveer advertencia de un ataque desde el cielo, Estados Unidos y sus aliados también pueden vigilar conjuntamente las redes de computadoras en busca de intrusiones.

Algunas de las defensas de computadoras de Estados Unidos ya están enlazadas con las de sus aliados, especialmente mediante asociaciones existentes de inteligencia de señales, pero se necesitan mayores niveles de cooperación para mantenerse a la delantera de la ciberamenaza. Se deben efectuar acuerdos más sólidos para propiciar el intercambio de información, tecnología e inteligencia con una mayor cantidad de aliados. En el informe OTAN 2020, un estudio encargado por la OTAN y presidido por la ex Secretaria de Estado de EE.UU., Madeleine Albright, se identificó con toda razón la necesidad de un nuevo "concepto estratégico" para la alianza para incorporar la ciberdefensa. El gobierno de Estados Unidos debe cerciorarse que la OTAN dedique más recursos a la ciberdefensa de manera que los estados miembros puedan defender redes que son parte integral de las operaciones de la alianza.

APROVECHANDO EL DOMINIO

Estados Unidos disfruta de recursos tecnológicos incomparables, y puede ordenar sus ventajas para crear capacidades militares superiores en el ciberespacio. El Pentágono ya ha comenzado a explorar cómo las compañías importantes pueden ayudar al sector público a tratar la ciberamenaza. Mediante una asociación pública-privada conocida como *Enduring Security Framework* (Marco de seguridad duradero), ahora los directores ejecutivos y los directores de tecnología de las compañías importantes de tecnología de informática y de la defensa se reúnen con regularidad con altos funcionarios del Departamento de Seguridad Nacional, de la Oficina del Director de Inteligencia Nacional y del Departamento de Defensa.

Las instituciones de investigación y desarrollo del gobierno de EE.UU. también han comenzado a prestarle atención a la ciberseguridad. Una de las innovaciones más importantes que ha surgido es el programa *National Cyber Range* (Campo Cibernético Nacional), elaborado por la Agencia de Investigación de Proyectos Avanzados de la Defensa (DARPA). Aunque la milicia estadounidense hace que las unidades lleven a cabo ejercicios de rutina en campos objetivos y en una variedad de simulaciones, el Pentágono no ha tenido esa capacidad cuando se trata de la ciberguerra. Es por ello que DARPA, que ayudó a inventar la *Internet* hace décadas, está elaborando el Campo Cibernético Nacional—de hecho, un modelo de la *Internet*—que le permitirá a la milicia a poner a prueba sus capacidades de ciberdefensa antes de ponerlas en uso. Las simulaciones también son relevantes para comprender el *software* malicioso concebido para infiltrar los sistemas de computadoras. Los laboratorios nacionales del Departamento de Energía han desarrollado granjas de computadoras que funcionan como placas de Petri, capturando viruses vivos de la *Internet* y observando cómo se propagan. Esas capacidades de entrenamiento y diagnóstico pueden ayudar a Estados Unidos a mantenerse a la cabeza de las ciberarmas innovadoras de sus adversarios.

DARPA está llevando a cabo investigaciones aún más fundamentales que podrían mejorar la capacidad del gobierno de atribuir ataques y entorpecer las capacidades de los intrusos, por ende tornando al ciberespacio en un entorno donde domine menos la ofensiva. La agencia también está retando a la comuni-

dad científica a que vuelva a analizar el diseño básico de la arquitectura de la red del Pentágono de manera que la milicia pueda rediseñar o actualizar el *hardware*, los sistemas operativos y los lenguajes de computadora con la ciberseguridad en mente. La infraestructura compleja de la tecnología de la informática no cambiará de la noche a la mañana, sino durante el transcurso de una generación, Estados Unidos cuenta con una verdadera oportunidad para ingeniárselas y salirse de la mayoría de las vulnerabilidades problemáticas de la tecnología de hoy.

El gobierno también debe fortalecer su capital de recursos humanos. El Pentágono ha aumentado la cifra de profesionales capacitados en ciberseguridad y ha profundizado su entrenamiento. Esto incluye un programa oficial de certificación del cual egresan anualmente tres veces la cantidad de profesionales en ciberseguridad al igual que años atrás. Siguiendo las prácticas de la industria, los administradores de la red del Pentágono ahora están capacitados en el "*hacking* ético", que incluye emplear técnicas adversas contra los propios sistemas de Estados Unidos para poder identificar los puntos débiles antes de que un enemigo se aproveche de ellos.

Inclusive a medida que el gobierno estadounidense fortalece su grupo de profesionales en ciberseguridad, debe reconocer que las tendencias a largo plazo en el capital de recursos humanos no son un buen presagio. Estados Unidos cuenta con tan sólo el 4,5 por ciento de la población del mundo, y durante los próximos 20 años muchos países, incluyendo a China e India, perfeccionarán a científicos en computadoras mucho más competentes de los que Estados Unidos capacitará. Estados Unidos perderá su ventaja en el ciberespacio si esa ventaja se predica en sencillamente acumular profesionales de ciberseguridad capacitados. Por lo tanto, el gobierno de EE.UU., debe enfrentar el reto de la ciberdefensa de la misma manera que enfrenta otros retos militares: con un enfoque no en las cifras sino en la tecnología superior y la productividad. Sensores de gran velocidad, la analítica avanzada y los sistemas automatizados serán necesarios para apoyar a los profesionales de ciberseguridad capacitados en la milicia estadounidense. Y esas herramientas solamente estarán disponibles si el sector comercial de la tecnología de informática de EE.UU. permanece como el líder mundial—algo que exigirá inversiones continuas en la ciencia, tecnología y educación a todos los niveles.

Hacer uso de la capacidad innovadora del sector privado también exigirá mejoras dramáticas en los procedimientos del gobierno para adquirir tecnología de informática. Por lo general, al Pentágono le toma 81 meses lograr que un sistema de computadora sea operacional después de haberse financiado. Tomando en consideración el crecimiento de la capacidad de la informática sugerido por la ley de Moore, esto significa que para cuando se entreguen los sistemas ya estarán como mínimo cuatro generaciones atrasadas a la última generación. Eso es menos tiempo de lo que le tomaría al Pentágono preparar un presupuesto y recibir la aprobación del Congreso.

Para poder duplicar el dinamismo de la industria privada, el Pentágono está creando una ruta de adquisición específica para la tecnología de la informática. Se basa en cuatro principios. Primero, la rapidez debe ser una prioridad crítica. El proceso de adquisición del Pentágono tiene que ser acorde con el ciclo de desarrollo de la tecnología. Con la tecnología de la informática, esto significa ciclos de 12 ó 36 meses, no siete u ocho años. Segundo, el Pentágono debe implementar desarrollo y pruebas en incrementos en lugar de tratar de desplazar sistemas grandes complejos "de golpe". Tercero, la milicia estadounidense debe estar dispuesta a sacrificar o aplazar la personalización para poder lograr mejoras rápidas en incrementos. Cuarto, las necesidades de la tecnología de informática del Departamento de Defensa—que van desde modernizar sistemas nucleares de mando y control hasta actualizar *software* de procesamiento de palabras—exigen diferentes niveles de demanda. Un método para la adquisición de tecnología de informática que abarque esos principios es esencial para la eficacia de la milicia de Estados Unidos cuando se trata de la ciberdefensa.

ENTRANDO A UNA NUEVA ERA

Los retos intimidantes de la ciberseguridad representan el inicio de una nueva era tecnológica. En esta primera hora, el punto más fuerte de Estados Unidos es su conocimiento de la transformación. La disyuntiva de hoy me hace recordar una carta urgente dirigida al Presidente Franklin Roosevelt en la víspera de otra nueva era tecnológica. Con fecha del 2 de agosto de 1939, dicha carta reza en parte, "Ciertos aspectos de la situación que ha surgido parecen exigir vigilancia y, de ser necesario, acción rápida por parte de la Administración. Por lo tanto creo que es mi deber informarles los siguientes hechos y recomendaciones". La carta fue firmada, "Atentamente, Albert Einstein". La advertencia de Einstein de que grandes avances en la fisión nuclear podrían hacer posible una bomba atómica llevó a Roosevelt a lanzar el Proyecto Manhattan, que ayudó a Estados Unidos a prepararse para la era atómica.

La ciberamenaza no involucra las implicaciones existenciales marcadas por la era nuclear, pero hay similitudes importantes. Los ciberataques ofrecen un medio para que posibles adversarios venzan las ventajas aplastantes de Estados Unidos en el poder militar convencional y para ello hay formas que son instantáneas y extremadamente difíciles de rastrear. Puede que esos ataques no causen las bajas en masa de un ataque nuclear, pero del mismo modo podrían paralizar la sociedad estadounidense. A la larga, la penetración sistemática de los *hackers* de los negocios y universidades estadounidenses podría robarle a Estados Unidos su propiedad intelectual y su ventaja competitiva en la economía global.

Estos riesgos son los que están obligando al Pentágono a forjar una nueva estrategia para la ciberseguridad. Los elementos principales de esa estrategia son desarrollar un modelo organizacional para el adiestramiento, equipamiento y comando de fuerzas de ciberdefensa; emplear protecciones en etapas con un fuerte núcleo de defensas activas; emplear las capacidades militares para apoyar las iniciativas de otros departamentos para asegurar las redes que administran la infraestructura crítica de Estados Unidos; forjar defensas colectivas con los aliados de Estados Unidos e invertir en el desarrollo rápido de capacidades adicionales de ciberdefensa. La meta de esta estrategia es hacer que el ciberespacio sea seguro de manera que sus innovaciones revolucionarias puedan realzar tanto la seguridad nacional como la seguridad económica de Estados Unidos. ❑

William J. Lynn III, es el trigésimo Secretario Adjunto de Defensa. Egresado del Dartmouth College, el Sr. Lynn cuenta con un doctorado en leyes de la Cornell Law School y una maestría en asuntos públicos de la Woodrow Wilson School en la Princeton University. La carrera profesional del Sr. Lynn incluye extensos servicios públicos en varios niveles dentro del gobierno. El Sr. Lynn se desempeñó en calidad de Subsecretario de la Defensa (Contraloría) desde 1997 hasta el 2001 y cuatro años antes de ello fue el Director de Análisis y Evaluación de Programas (PA&E) en la Oficina del Secretario de Defensa. Antes de pasar a formar parte del Departamento de Defensa en 1993, el Sr. Lynn sirvió durante seis años en la plantilla del Senador Edward Kennedy en calidad de enlace en el Comité de Servicios Armados del Senado. Antes de 1987, fue becado superior en la National Defense University y formaba parte de la plantilla profesional del Institute for Defense Analyses (Instituto para Análisis de la Defensa).