

AGENDA

DE LA POLITICA EXTERIOR DE LOS ESTADOS UNIDOS DE AMERICA

Volumen 3

Periódicos Electrónicos del Servicio Cultural e Informativo de los Estados Unidos

Número 2

*LA AMENAZA CIBERNETICA
LA PROTECCION DE LAS REDES
ESTADOUNIDENSES*



Noviembre de 1998

AGENDA

DE LA POLÍTICA EXTERIOR
DE LOS ESTADOS UNIDOS DE AMERICA

LA AMENAZA CIBERNÉTICA — LA PROTECCIÓN DE LAS REDES DE INFORMACIÓN ESTADOUNIDENSES

AGENDA DE LA POLÍTICA EXTERIOR DE LOS ESTADOS UNIDOS, VOLUMEN 3, NUMERO 2, Junio de 1998



“Según nos aproximamos al siglo XXI, nuestros enemigos han ampliado los campos de batalla del espacio físico al espacio cibernético... En lugar de invadir nuestras playas o enviar bombarderos, estos adversarios pueden intentar ataques cibernéticos contra nuestros sistemas militares esenciales y nuestra base económica... Si nuestros hijos han de crecer a salvo y libres, debemos enfocar esas nuevas amenazas del siglo XXI con el mismo rigor y determinación que empleamos contra los retos a nuestra seguridad más severos de este siglo”

***Presidente Clinton
Discurso en la Graduación de la Academia Naval de Estados Unidos
22 de mayo de 1998***

Este número de “Agenda de Política Exterior de Estados Unidos” examina la respuesta de Estados Unidos a los retos nunca encontrados hasta ahora — retos que son exclusivos de la Edad de la Informática. Funcionarios estadounidenses claves explican las iniciativas encaminadas a proteger las redes de información estadounidenses de un ataque cibernético y promover la cooperación entre el gobierno y el sector privado en el desarrollo de medidas de seguridad. Un senador estadounidense ofrece la reacción congresional al debate sobre la guerra de la informática, un miembro de los círculos académicos bosqueja cómo responden las universidades a las prioridades nacionales en surgimiento, un experto del sector privado ofrece un panorama amplio del significado y evolución de la guerra de la informática, y especialistas en seguridad del sector privado exponen perspectivas sobre cómo las compañías estadounidenses trabajan entre sí y con el gobierno para cumplir con los requisitos de seguridad de la era cibernética.

AGENDA
DE LA POLITICA EXTERIOR
DE LOS ESTADOS UNIDOS DE AMERICA
LA AMENAZA CIBERNETICA – LA PROTECCION
DE LAS REDES DE INFORMACION ESTADOUNIDENSES

CONTENIDO

ENFOQUE

LA DEFENSA DE LA NACION ANTE UN ATAQUE CIBERNETICO: LA SEGURIDAD INFORMATICA EN EL MUNDO DE HOY	5
Por el teniente general Kenneth A. Minihan Director de la Agencia de Seguridad Nacional de Estados Unidos (NSA)	
LA SEGURIDAD INFORMATICA Y LA NUEVA EPOCA DE SEGURIDAD NACIONAL	9
Por el doctor John Hamre Vicesecretario de Defensa	
CIAO: ENFOQUE INTEGRADO PARA CONTRARRESTAR LAS AMENAZAS DE UNA "NUEVA ERA"	12
Entrevista con el doctor Jeffrey A. Hunker, Director de la Oficina de Seguridad de la Infraestructura Esencial	
EL PROBLEMA DEL AÑO 2000	18
Por John Koskinen Presidente del Consejo Presidencial para la Conversión del Año 2000	
LA AMENAZA DE LA GUERRA INFORMATICA REQUIERE MAYOR ATENCION EN TODOS LOS FRENTES	20
Entrevista con el senador Jon Kyl	
COMENTARIO	
¿FANTASMAS EN LAS MAQUINAS?	24
Por el doctor Martin Libicki Analista de políticas principal, RAND	
LA RESPUESTA DE LA EDUCACION SUPERIOR A LA GUERRA DE LA INFORMACION	28
Por el doctor Charles W. Reynolds Director del Departamento de Informática y Decano Interino del Colegio de Ciencias y Tecnología Integradas, de la Universidad James Madison	
OPINIONES DEL SECTOR PRIVADO	
LOS SECTORES PRIVADOS Y PUBLICOS SE BENEFICIAN AL COMPARTIR SU EXPERIENCIA EN ASUNTOS DE SEGURIDAD	34
Entrevista con Howard Schmidt, director de Seguridad Informática de Microsoft Corporation	
ESTRATEGIAS PARA CONTRARRESTAR LAS AMENAZAS A LOS RECURSOS DE TECNOLOGIA DE INFORMACION	38
Por James A. Lingerfelt Consultor principal, IBM, Seguridad Pública y Justicia	

LA GUERRA INFORMATICA: DESAFIO Y OPORTUNIDAD	45
Por James Adams	
Director de Infraestructura Defense, Inc.	
ANTECEDENTES DEL TEMA	
FACT SHEET: PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES	49
Presidential Decision Directive 63	
GUIA DE LECTURAS ADICIONALES	
LA AMENAZA CIBERNETICA: LA PROTECCION DE LAS REDES DE INFORMACION ESTADOUNIDENSES — ALERTA DE ARTICULOS	50
Extractos de artículos recientes	
LA AMENAZA CIBERNETICA: LA PROTECCION DE LAS REDES DE INFORMACION ESTADOUNIDENSES — BIBLIOGRAFIA	53
Se destacan otras opiniones	
LA AMENAZA CIBERNETICA: LA PROTECCION DE LAS REDES DE INFORMACION ESTADOUNIDENSES — SITIOS CLAVES EN LA INTERNET	54
Vínculos en la Internet con recursos sobre temas relacionados	

AGENDA

DE LA POLITICA EXTERIOR DE LOS ESTADOS UNIDOS DE AMERICA

Los periódicos electrónicos del USIS, publicados y transmitidos a todo el mundo a intervalos de tres semanas, examinan temas importantes que encaran Estados Unidos y la comunidad internacional, e informan al público extranjero acerca de Estados Unidos. Los periódicos — PERSPECTIVAS ECONOMICAS, TEMAS MUNDIALES, TEMAS DE LA DEMOCRACIA, AGENDA DE POLITICA EXTERIOR DE ESTADOS UNIDOS Y SOCIEDAD Y VALORES ESTADOUNIDENSES — brindan análisis, comentario e información de antecedentes en sus respectivas áreas temáticas. Todos los periódicos aparecen en versiones en inglés, francés y al español; algunos temas seleccionados aparecen también en árabe, portugués y ruso.

Las opiniones expresadas en los periódicos no reflejan necesariamente los puntos de vista o políticas del gobierno de Estados Unidos. Se ruega observar que USIS no asume responsabilidad por el contenido y acceso continuo a los sitios en la Internet relacionados con los periódicos electrónicos; tal responsabilidad recae totalmente en los proveedores. Los artículos pueden reproducirse y traducirse fuera de Estados Unidos, a menos que haya restricciones específicas de derechos de autor.

Los números actuales o atrasados de los periódicos pueden encontrarse en la página del Servicio Informativo y Cultural de Estados Unidos (USIS) en la World Wide Web en "<http://www.usia.gov/journals/journals.htm>". También están disponibles en varios formatos electrónicos para facilitar la observación en la pantalla, la transferencia, descarga e impresión. Se agradece cualquier comentario en su oficina local del USIS o en las oficinas editoriales:

Editor, U.S. Foreign Policy Agenda
Political Security (I/TPS)
U.S. Information Agency
301 4th Street, SW
Washington, D.C. 20547
United States of America.

Es posible también comunicarse vía email en el:

ejforpol@usia.gov

Se ruega observar que este número de AGENDA DE POLITICA EXTERIOR DE ESTADOS UNIDOS se encuentra en la página de USIS en la World Wide Web en "<http://www.usia.gov/journals/itps/1198/ijpe/ijpe1198.htm>".

Editor	Leslie High
Directora	Dian McDonald
Editores asociados	Wayne Hall
.....	Guy Olson
Redactores colaboradores	Ralph Dannheisser
.....	Susan Ellis
.....	Margaret A. McKay
.....	Jody Rose Platt
.....	Jacqui S. Porth
Especialistas en consulta	Rebecca Ford Mitchell
.....	Vivian Stahl
Director de arte	Barbara Long
Ayudante Gráfica	Sylvia Scott
Junta Editoria	Howard Cincotta
.....	Rosemary Crockett
.....	John Davis Hamill

LA DEFENSA DE LA NACION ANTE UN ATAQUE CIBERNETICO: LA SEGURIDAD INFORMATICA EN EL MUNDO DE HOY

Por el teniente general Kenneth A. Minihan
Director de la Agencia de Seguridad Nacional de Estados Unidos (NSA)

En muchas situaciones, las operaciones de mantenimiento de la paz de las Naciones Unidas le permiten a Estados Unidos ejercer "influencia sobre los acontecimientos, sin asumir todo el peso del costo y del riesgo", dice Hull. Los estadounidenses "tienen profundo interés en que los conflictos se contengan, los disturbios sociales se reduzcan al mínimo y se respeten las pautas de conducta internacional.... Es preciso que retengamos la flexibilidad de poder emplear el mantenimiento de la paz de las Naciones Unidas como una alternativa viable" para responder a las emergencias internacionales. Hull es director de la Oficina de Operaciones de Mantenimiento de la Paz y Humanitarias de la División de Asuntos de Organizaciones Internacionales del Departamento de Estado de Estados Unidos.

"Estamos en peligro. Norteamérica depende de las computadoras. Estas controlan la distribución de la energía, las comunicaciones, la aviación y los servicios financieros. Las computadoras se utilizan para guardar información vital: desde archivos médicos hasta planes de empresas y expedientes penales. Y aunque confiamos en ellas, pueden fallar, ya sea debido a un mal diseño o a un control de calidad deficiente, o a accidentes y, lo que todavía es peor, debido a una agresión deliberada. El ladrón de hoy puede robar más cosas con una computadora que con un revólver. El terrorista del mañana podrá hacer más daño con un teclado de computadora que con una bomba".

"Computers at risk", Consejo de Investigación Nacional, 1991

Prólogo

Quizá lo que más sorprende de las palabras que arriba se citan, es que se escribieron casi en los albores de la era de la informática. Hasta hace poco nosotros, como nación, casi no les habíamos prestado atención. Estados Unidos, y el resto del mundo, continúa adentrándose de lleno en la revolución cibernética: la tecnología

de la informática incursiona profundamente en la misma trama de nuestra sociedad y en nuestra economía como una nación la comunidad mundial. Realmente, la "super carretera de la información" se ha convertido en el elemento económico vital de nuestra nación.

Aunque Estados Unidos lidera al mundo en la era de la informática, el país se ha vuelto especialmente dependiente de la tecnología informática: de las computadoras y de la red mundial que las conecta. Esta dependencia se ha convertido en una clara y apremiante amenaza a nuestro bienestar económico, a nuestra seguridad ciudadana y a nuestra seguridad nacional.

Las redes del mundo, que muchos llaman "ciberespacio", no saben de fronteras físicas. Nuestra capacidad cada vez mayor de conectarnos a través del ciberespacio nos deja cada vez más expuestos a nuestros adversarios de toda la vida y de un creciente número de nuevos adversarios. Los terroristas, los grupos radicales, los narcotraficantes y el crimen organizado se unirán a las naciones-estado adversarias para aprovechar una creciente serie de medios informáticos de agresión avanzados. Las agresiones cibernéticas complementarán o

reemplazarán las tradicionales agresiones militares, lo cual complicará y exacerbará las vulnerabilidades que debemos prevenir y combatir. Entre los recursos que corren riesgo se encuentra no sólo la información que se almacena o que recorre el ciberespacio, sino además todos los componentes de nuestra infraestructura nacional que dependen de la tecnología de la informática y de la disponibilidad oportuna de información exacta. Estos incluyen la infraestructura de las telecomunicaciones misma; nuestros sistemas bancario y financiero; nuestro sistema de energía eléctrica; otros sistemas de energía, como los oleoductos y los conductos de gas natural; nuestras redes de transporte; los sistemas de distribución de agua; los sistemas médicos y de salud; los servicios de emergencia, como la policía, los bomberos y los cuerpos de rescate, y el funcionamiento del gobierno a todos los niveles. Todos éstos son necesarios para el éxito económico y la seguridad nacional.

Seguridad de información: la meta nacional

En 22 de mayo de 1998, el presidente firmó la Directiva de Decisión Presidencial 63 (PDD-63) sobre la Protección de la Infraestructura Crítica. En ésta señala: "Mi intención es que Estados Unidos tome todas las medidas necesarias para eliminar con prontitud cualquier vulnerabilidad significativa a las agresiones tanto físicas como cibernéticas contra nuestras infraestructuras críticas, especialmente nuestros sistemas cibernéticos.

La meta nacional es que, para el año 2000, a lo sumo, Estados Unidos haya logrado una capacidad operativa inicial, y que para dentro de 5 años, a más tardar, Estados Unidos haya logrado y pueda mantener la capacidad de proteger las infraestructuras críticas de nuestra nación de actos intencionales que debilitarían considerablemente la capacidad de:

- el gobierno federal de desempeñar las misiones esenciales de seguridad nacional y garantizar la salud y seguridad de los ciudadanos;
- los gobiernos estatales y locales de mantener el orden y proporcionar un mínimo esencial de servicios públicos.
- el sector privado de asegurar el funcionamiento ordenado del sistema económico y proporcionar

servicios esenciales de telecomunicaciones, energía, financieros y de transporte.

El logro de esta abarcadora meta significará un esfuerzo considerable, que necesitará la cooperación entre el gobierno y los elementos del sector privado que manejan las infraestructuras críticas. La PDD instruye al gobierno federal que dé ejemplo asegurando la confiabilidad de los sistemas federales, pero también aclara que el sector público no puede resolver el problema de forma unilateral. Todos los departamentos y agencias federales dependen sobremedida de los servicios proporcionados por el sector privado: energía, telecomunicaciones, transporte, etc. Por lo tanto, la PDD prevee una Asociación Pública y Privada para desarrollar y poner en práctica un Plan Nacional de Seguridad de la Infraestructura, para resolver la amenaza del terrorismo electrónico. El punto principal radica en cómo lograr que el sector privado se comprometa con el Plan de Seguridad de la Infraestructura desde una perspectiva nacional. Debido a la gran competitividad actual, el sector privado tiende por lo general a buscar las ventajas en el mercado — incluyendo la reducción de los costos operativos — para aumentar las utilidades. El logro de mejores medidas de protección cibernética requerirá tanto una mayor inversión como una colaboración entre competidores.

Elementos esenciales

Cualquier estrategia que haga que nuestras Infraestructuras Críticas sean más fiables (resistentes) debe comprender tres elementos básicos: una mayor protección frente a las agresiones cibernéticas, la capacidad de detectar cuándo ocurre una agresión y la capacidad de responder y recuperarse cuando una agresión ha sido detectada.

La protección frente a la agresión cibernética se basa en la tecnología del cifrado de datos — incluyendo las firmas codificadas digitalmente — la cual proporciona servicios de autenticación, integridad, prevención de la posibilidad del repudio y privacidad y confidencialidad necesarios para garantizar la información. Quizá la mejor arma de protección contra la agresión cibernética sea la autenticación basada en la codificación digital que se emplea para dar acceso a la información. El cifrado se emplea en

computadoras, en los servidores y en todas las redes para asegurar que la información referente a asuntos confidenciales de gobierno y de particulares se mantenga en esas condiciones. La tecnología del cifrado, que antaño fue patrimonio exclusivo de los gobiernos, se distribuye hoy libremente en el mercado y constituye un garantizador básico de la seguridad de información. De hecho, el 16 de septiembre de este año, el vicepresidente anunció que se llevaría a cabo una actualización general de la Política de Control de Exportación de Estados Unidos sobre la Tecnología del Cifrado, lo cual es una clara indicación de la importancia del cifrado en la protección de la infraestructura crítica, así como en el comercio electrónico mundial y la prosperidad económica.

Dado que la tecnología de cifrado ya es un hecho, el siguiente objetivo es utilizarla de un modo coherente y eficaz en todas nuestras infraestructuras críticas. Para hacer esto hace falta establecer un marco donde el cifrado se pueda emplear a diferentes niveles y de modo interoperativo (es decir, que pueda funcionar en distintos sistemas informáticos) y, al mismo tiempo, hace falta establecer una infraestructura de claves públicas (PKI) que provea firmas digitales y certificados de claves de cifrado que sean fiables y reconocibles a nivel mundial: “la identificación electrónica” particular y exclusiva de la era de la informática. Los servicios de PKI surgen en el sector privado para satisfacer la demanda del comercio electrónico a nivel mundial y pueden adaptarse para proporcionar protección a la infraestructura crítica.

En cuanto al diagnóstico, detección y respuesta a la agresión cibernética, la tecnología no está tan avanzada ni es tan efectiva. Hoy día, Estados Unidos tiene muy poca capacidad de detectar o reconocer una agresión cibernética dirigida a las infraestructuras del gobierno o del sector privado, y todavía tiene menos capacidad de respuesta. La capacidad de identificar una agresión cibernética estratégica contra a uno o varios componentes de la infraestructura crítica, y responder de un modo apropiado, es claramente un tema de seguridad nacional importante. Uno de los factores que complica la situación es el hecho de que tradicionalmente los intrusos que interfieren con las computadoras se han considerado delincuentes que incumben a las agencias encargadas de ejecutar la ley. Cuando

aparece alguno, es de esperar que se lo rastree, detenga y enjuicie. Además, el sector privado no ha estado muy dispuesto a compartir información sobre algún caso de intrusión en sus sistemas computarizados, por miedo de recibir mala prensa (v.g., titulares en los diarios tales como: “Se estima en millones las pérdidas bancarias en allanamiento de computadoras” o “Piratas cibernéticos dislocan el servicio telefónico”) y por la reacción del público. Para llegar a tener una capacidad de defensa nacional efectiva frente a las agresiones cibernéticas, han de crearse nuevas normas de acción recíproca que permitan la colaboración abierta y dinámica entre el sector privado, las fuerzas policiales y la comunidad de seguridad nacional.

Función de la Agencia de Seguridad Nacional en la seguridad de la información

En la era de la informática, las misiones tradicionales de la Agencia de Seguridad Nacional (NSA) — inteligencia de comunicaciones y seguridad de sistemas de información — confluyen en una: proporcionar superioridad de información a Estados Unidos y sus aliados. Teniendo en cuenta este esquema, es fundamental comprender bien la Infraestructura de Información Mundial y las vulnerabilidades de los Sistemas de Información de Redes ante las agresiones cibernéticas. Desde una postura defensiva, la NSA ha llevado a cabo una serie de iniciativas para establecer la base técnica para proteger nuestras infraestructuras críticas.

Como antes mencioné, la tecnología del cifrado es de dominio público y constituye la principal fuente de protección de los sistemas de información en caso de una agresión cibernética. Lo malo es que hay muchos productos en el mercado que no pueden funcionar de forma segura en distintos sistemas informativos y varían en cuanto a su robustez, y, además, hay muchas maneras, a menudo confusas, de cifrar datos. Por ejemplo, está por un lado el cifrado del correo electrónico, el cifrado de archivos, el cifrado de la web o servidor de información, el cifrado de enlaces y el cifrado de redes virtuales privadas, entre otros. Para solucionar esta situación, la NSA se ha asociado con los principales proveedores de tecnología para facilitar la seguridad en la información con el fin de desarrollar un marco común de servicios de cifrado y proveer soluciones a la seguridad de

información que incluyan al sector privado. Este marco establece un modo coherente de utilizar la tecnología del cifrado en el sector privado, al mismo tiempo que define cómo dicho cifrado interactúa y apoya otras tecnologías y productos relacionados con seguridad; v.g.: cortafuegos, servidores, routers, sistemas operativos, detección de intrusos, detección de códigos dañinos, dispositivos auditivos, y servicios de infraestructura de claves públicas (PKI).

Otro aspecto del problema es el de los diferentes grados de fiabilidad en muchos de los productos de seguridad que se le venden al público. Para tratar de resolver este problema, la NSA se ha asociado con el Instituto Nacional de Estándares y Tecnología (NIST). Este acuerdo establece que la NSA y el NIST comisionarán los servicios de diferentes laboratorios privados para que evalúen los productos relacionados con la seguridad cibernética que hayan salido al mercado, ya sea con el fin de avalar las aseveraciones del fabricante, o para cerciorarse de que se atengan a los requisitos definidos en el marco de la seguridad de redes. La revisión de los productos la llevarán a cabo diversos laboratorios certificados que serán remunerados de acuerdo con los servicios que presten; el costo y el ritmo del trabajo se acordarán mediante negociaciones entre el laboratorio y el fabricante del producto.

Por último, la Agencia de Seguridad Nacional opina que la nación necesita compartir una serie de elementos que garanticen la seguridad de la información nacional y destina recursos a fin de desarrollar la tecnología necesaria para crear un

sistema nacional de detección y respuesta ante una agresión cibernética. Este modelo integra una variedad de sensores que pueden colocarse en lugares críticos de la infraestructura y en la infraestructura de telecomunicaciones misma, y comprende técnicas analíticas avanzadas y de amplio alcance para proveer un panorama dinámico de cualquier amenaza a las infraestructuras críticas desde el ciberespacio mundial. Estas técnicas deben compartirse entre los diferentes componentes nacionales: los de seguridad nacional, federal, industrial y regional, para que, concurrentemente, puedan detectar, defender, reconstituir y recuperar los servicios vitales.

Conclusión

La prosperidad económica de que hoy disfruta nuestra nación, se debe en gran parte a la era de la informática y a nuestro liderazgo mundial en el campo de la tecnología de la informática. Nuestro continuo liderazgo y prosperidad en el campo de la economía mundial puede muy bien depender de nuestro compromiso nacional de actuar como líderes y proporcionar integridad y responsabilidad — seguridad de información — en el ámbito de la informática mundial, con cuya creación hemos contribuido. En su mensaje al emitir la PDD-43, el gobierno ha dejado bien patente que es el momento de actuar, y que la NSA se encuentra lista para apoyar dicha responsabilidad con nuestro conocimiento técnico. La superioridad en el campo de la información en la era de la informática es un claro imperativo nacional.

LA SEGURIDAD INFORMATICA Y LA NUEVA EPOCA DE SEGURIDAD NACIONAL

**Por el doctor John Hamre
Vicesecretario de Defensa**

(Proteger los recursos de información esenciales será “uno de los retos que determinarán la seguridad nacional en los años venideros”, afirma el vicesecretario de Defensa John Hamre. Al señalar que el Pentágono es responsable de proteger 28.000 sistemas diferentes de computación, el vicesecretario advierte que proteger al mundo virtual de las amenazas cibernéticas “es tanto un proceso de planteamiento administrativo y de atención como de tecnología”).

Estados Unidos ha enfrentado cinco épocas de seguridad nacional, en las que cada cambio involucró transiciones desde un pasado cierto a un futuro incierto. La primera época abarcó el período desde la Guerra Revolucionaria hasta mediados de la década de 1820, cuando Estados Unidos se encontraba en la periferia de un entorno de seguridad internacional dominado todavía por Europa.

Desde mediados de la década de 1830 hasta el final del siglo XIX, disfrutamos del aislamiento que nos proveía el Océano Atlántico para atender nuestros propios asuntos, mientras la vieja estructura política europea se desintegraba. Esta segunda época terminó con la Primera Guerra Mundial y el surgimiento de la Unión Soviética. Una tercera época tuvo lugar desde 1920 hasta 1946, la que se caracterizó por una recesión mundial y el ascenso del comunismo internacional, mientras Europa se desplomaba. Estos acontecimientos causaron una crisis en la democracia norteamericana y su sistema de libre empresa, con la Gran Depresión, y las tensiones en el entorno de la seguridad internacional culminaron finalmente en la Segunda Guerra Mundial. La época más reciente — la Guerra Fría — fue dominada por un mundo bipolar. Estados Unidos encabezó la comunidad internacional en la creación de instituciones para reconstruir las economías arruinadas de Europa y abordar el derrumbe de los viejos imperios europeos en el Tercer Mundo. Al mismo tiempo,

Estados Unidos lideró el mundo libre para contener al comunismo, hasta el derrumbe de la Unión Soviética.

Ahora nos encontramos en transición hacia una época nueva, aparentemente caracterizada por el renacimiento de antiguos peligros: nacionalismo y orgullo étnico. Otra dimensión de esta época nueva es la disolución del control y la propagación de las tecnologías que fueron creadas en la época última y el ascenso espectacular de nuevas y extraordinarias capacidades técnicas que poseen un potencial, hasta ahora sin precedente, tanto para el bien como el mal. Vivimos ahora con el temor inquietante de “misiles nucleares sin control” y armas químicas y biológicas en manos de terroristas.

La próxima época de seguridad nacional también nos presentará el reto de la seguridad cibernética. El crecimiento explosivo en la utilización de tecnologías informáticas ha tenido un efecto profundo en todos los sectores de la economía y el gobierno norteamericanos. La tecnología informática ha incentivado un crecimiento económico asombroso, ha mejorado en forma drástica las comunicaciones, y permitió a las empresas norteamericanas competir más eficazmente que nunca. Estados Unidos — y el mundo — dependen en efecto de la tecnología informática, en formas inimaginables hasta apenas unos pocos años atrás.

En ninguna parte esto es más cierto que en las fuerzas militares norteamericanas. El Departamento de Defensa (DOD) utiliza la tecnología informática para realizar lo que llamamos una Revolución en los Asuntos Militares — el movimiento y uso de grandes cantidades de información para proveer inteligencia más confiable, mando y control radicalmente mejorados, mejores prácticas comerciales, y sistemas de armas más poderosas. Esta revolución es vital si queremos seguir preparados para defender hoy los intereses norteamericanos y prepararnos para la amenaza de la próxima época de seguridad nacional.

La revolución de las tecnologías informáticas toca a cada rincón del Departamento de Defensa, tanto en el terreno de operaciones como en la sede central. Muy pronto nuestros soldados a nivel de pelotón tendrán comunicaciones que permitirán a los comandantes conocer exactamente la posición, situación, y hasta el ritmo cardíaco de cada soldado en particular — casi un “conocimiento completo del teatro de operaciones”. Nuestros marinos envían correo electrónico desde barcos en alta mar luego de utilizar una tecnología muy similar para coordinar el objetivo de los misiles cruceros. Los pilotos incluyen ahora la “saturación de misión” del caudal de información de que disponen mientras están en vuelo.

En nuestros procesos logísticos, se emplea la tecnología para conectar las líneas de batalla con las líneas de abastecimiento. Para fin del siglo estamos nos hemos comprometido a llegar a un proceso de compras libre de papeleo. Hemos abierto nuestra Oficina de Programas Electrónicos Conjuntos para modernizar las compras a nivel de unidad y utilizamos ahora los “centros comerciales” electrónicos de la Internet para comprar de todo, desde lapiceros a activadores hidráulicos. Utilizamos la Internet para una serie de funciones que abarcan desde el pago de gastos de viaje a comunicaciones por satélite, y hemos hecho adelantos enormes en la preparación electrónica de publicaciones.

En pocas palabras, el Departamento de Defensa aprovecha el poder de las microfichas para crear las fuerzas armadas del siglo XXI. Sin embargo, al hacer esto también debemos reconocer que con las nuevas tecnologías surgen nuevos

peligros. Las mismas tecnologías que nos permiten buscar nuevos métodos más eficientes también pueden ser utilizadas por aquellos que no nos pueden atacar en el campo de batalla corriente pero que nos atacan en el espacio cibernético. Esto forma parte de una nueva dimensión muy diferente y muy importante del razonamiento acerca de la seguridad nacional; tecnologías y capacidades a las que anteriormente sólo tenían acceso los gobiernos de los países grandes, ahora están al alcance de los individuos. La protección de nuestros recursos informáticos — la seguridad informática — será por lo tanto uno de los retos que determinarán la seguridad nacional en los años venideros.

Hay poca duda en cuanto a que la seguridad informática es de importancia esencial; nosotros, en el Departamento de Defensa, ya hemos visto la primera ola de amenazas cibernéticas, tanto en ejercicios como en ataques reales. Para conocer la medida de nuestras vulnerabilidades, el año pasado realizamos un ejercicio. Nuestro “enemigo” fue un grupo de unas 35 personas cuya misión fue penetrar los sistemas de computadoras del Departamento de Defensa. Sus herramientas se limitaban a tecnologías obtenibles comercialmente y a programas de computadora vendidos en el mercado o recogidos en la Internet. En el transcurso de tres meses, el grupo, que operaba sujeto a esas limitaciones, fue capaz de atacarnos, de penetrar nuestras redes no confidenciales y, de hecho, hubiera podido trastornar gravemente nuestras comunicaciones y sistemas de fuerza.

En febrero pasado, sufrimos un ataque organizado contra los sistemas de computadoras del Pentágono, en un momento en que aumentábamos nuestro despliegue de fuerzas en el Golfo Pérsico. Resultó que el ataque fue obra de dos adolescentes de California, pero, al producirse en ese momento, pudo haber sido mucho más grave. Tanto nuestro ejercicio como los ataques en pequeña escala sirvieron para alertarnos de que al considerar ataques más graves no solamente debemos pensar “si ocurren”, sino “cuando y donde” pueden ocurrir.

Para hacer frente a estas amenazas, primero debemos considerar nuestra manera de pensar. Los norteamericanos, por tradición, hemos pensado en la seguridad como una cerca en

derredor de un patio, que establecía las fronteras y protegía el espacio interior. De romperse la cerca, se la puede arreglar y asegurar nuevamente. Este razonamiento dio buenos resultados en las épocas anteriores de seguridad nacional, pero en el espacio cibernético no hay fronteras. La transición hacia la época que vendrá tiene que distinguirse no solamente por el adelanto tecnológico, sino que también por la flexibilidad del razonamiento. Debemos reconocer que la seguridad en el mundo virtual es tanto un proceso de planteamiento administrativo y de atención como de tecnología.

Cambiar de manera de pensar puede ser una de las tareas más difíciles. Por ejemplo, sin darnos cuenta, en este momento suministramos a enemigos potenciales información para cuya adquisición se gastaron anteriormente cientos de millones de dólares en operaciones de inteligencia. Tuvimos una instalación militar que tenía lo que se creyó ser una excelente página principal en la Web. En ella aparecía una vista aérea de la instalación, con edificios identificados como "Centro de Operaciones" y "Centro de Apoyo Técnico". En términos de relaciones públicas la página era efectiva, pero también proveía valiosa información sobre un potencial blanco a aquellos que pudieran desear hacernos daño.

Conociendo las cuestiones más amplias involucradas en la seguridad informática, debemos tomar medidas tangibles para proteger nuestros recursos de información. El año pasado el Departamento de Defensa llevó a cabo diversos esfuerzos para tratar de comprender las exigencias de proteger nuestra infraestructura informática. El ritmo de los adelantos en la tecnología informática hace que éste sea un reto intimidante; el Departamento de Defensa mantiene 28.000 sistemas diferentes de computación, todos ellos puestos al día y cambiados periódicamente, y debemos conocer sus vulnerabilidades. El reto de la seguridad informática es semejante al de la guerra, y lo encaramos de esa manera al designar un Comandante Conjunto para la Defensa de Redes de Computadoras con el fin de organizar nuestros esfuerzos. El Departamento de Defensa también es contribuyente clave del Centro Nacional de Protección de la Información y en la Oficina de

Seguridad de Información Esencial, que depende de la Casa Blanca.

También se necesitan otras medidas. El noventa y cinco por ciento de nuestras comunicaciones se realiza ahora por líneas de teléfono y fax públicas, lo que hace que la criptografía sea un elemento principal de la seguridad informática. Uno de los casos hipotéticos más peligrosos en el mundo virtual es que nuestros combatientes reciban mensajes "engañosos" que los despisten. Por lo tanto, sin una criptografía confiable, toda la estructura informática de que dependemos es vulnerable. En respuesta a esta amenaza, trabajamos ahora para asegurar que dentro del Departamento de Defensa podamos garantizar la identidad digital de los usuarios y desarrollar un sistema público clave de confianza. Debemos fortalecer nuestros procesos criptográficos de modo que la información que transmitimos y manejamos electrónicamente sea segura y verificable.

El Departamento de Defensa también hace adelantos importantes en proveer una seguridad más amplia de las redes. Instalamos capacidades de vigilancia de redes y trabajamos para asegurar el control de la configuración en un entorno dinámico e inherentemente cambiante de las redes. Instalamos sistemas de prevención de acceso de intrusos, centros de vigilancia de redes, identificación digital, y una infraestructura de seguridad.

La seguridad informática, la criptografía y la seguridad de las redes, plantean algunos de los retos más difíciles que el Departamento de Defensa jamás haya enfrentado. Para hacer uso de la revolución de la técnica informática, debemos asegurar el acceso a los bienes de que dependemos así como también su protección. Damos pasos gigantescos para lograrlo, pero mucho queda por hacer. Las exigencias de estos días requieren que nos dirijamos a los profesionales de la información tanto del Departamento de Defensa como de los sectores gubernamentales y privados más amplios para proteger los sistemas que son vitales para todos nosotros. Debemos asegurar que el paso de nuestra nación por la nueva época de seguridad nacional sea tan exitoso como el de la última época.

CIAO: ENFOQUE INTEGRADO PARA CONTRARRESTAR LAS AMENAZAS DE UNA “NUEVA ERA”

**Entrevista con el doctor Jeffrey A. Hunker,
Director de la Oficina de Seguridad de la Infraestructura Esencial**

“El apoyo total del sector privado” es vital para la protección de la infraestructura esencial de Estados Unidos contra ataques cibernéticos, dice el doctor Jeffrey A. Hunker, director de la Oficina de Seguridad de Infraestructura Esencial (CIAO). “La amenaza a que nos enfrentamos es del tipo que aumenta con el tiempo”, dice. “De manera que tenemos que responder reconociendo la urgencia y llegar rápidamente a resultados reales para combatirla”. Hunker fue entrevistado por Susan Ellis, redactora colaboradora).

PREGUNTA: Como director de CIAO usted está a cargo de producir un plan nacional integrado para hacer frente a las amenazas físicas y cibernéticas contra las comunicaciones, el transporte, la energía y demás infraestructura esencial del país. ¿Cuál es la tarea más difícil e importante que encuentra en el cumplimiento de las nuevas responsabilidades que le corresponden en virtud de esta iniciativa anunciada por el presidente Clinton en mayo pasado?

HUNKER: El problema clave reconocido por el presidente consiste en que actualmente vivimos en una nueva era en la que existen amenazas que no habíamos experimentado antes. Específicamente, ahora vivimos en una época en la cual, como consecuencia de que las telecomunicaciones y la Internet están tan conectadas entre sí con nuestros sistemas de energía eléctrica y nuestros sistemas básicos de transporte y telecomunicaciones, estos sistemas son vulnerables al trastorno que pueden causar los que llamamos ataques cibernéticos, por medio de computadoras, utilizando la Internet para penetrar en forma irregular en los sistemas y desorganizarlos o desbaratarlos. Ese tipo de ataque podría no sólo interferir, por ejemplo, con operaciones militares, sino que podría interrumpir servicios vitales para la economía, y de los que dependen los estadounidenses, como la energía eléctrica, los teléfonos y los servicios básicos de transporte.

Es un problema totalmente nuevo que ha surgido gracias a la tecnología y la interconexión de la economía estadounidense. El problema básico a que nos enfrentamos es informar a los estadounidenses sobre esta nueva amenaza y colaborar con el sector empresarial y las industrias claves para asegurarnos de que efectivamente tengamos protección contra estos tipos de ataques cibernéticos.

P.: ¿Realmente es totalmente nuevo, verdad?

HUNKER: Sí. En los últimos 10 años hemos conectado con éxito los sectores económicos del país, lo que ha traído grandes beneficios en cuanto al crecimiento económico y la prosperidad de que Estados Unidos ha disfrutado. Sin embargo, con esa nueva prosperidad también ha llegado una nueva vulnerabilidad y, bien se trate de países o grupos terroristas o carteles delictivos que nos quieran hacer daño, esta nueva vulnerabilidad, nacida de nuestra dependencia de los sistemas electrónicos y de los sistemas basados en la información, es una nueva manera en que se nos puede atacar.

P.: ¿Cuáles son los organismos del gobierno que tratan de contrarrestar esta amenaza y en qué forma colabora su oficina con ellos para llevar a cabo su misión?

HUNKER: Hay 11 organismos principales del

gobierno federal a los cuales el presidente ha encargado trabajar juntos. Entre los claves están el Departamento de Defensa y organismos asociados; el sector de inteligencia y las autoridades encargadas de hacer cumplir la ley (la Oficina Federal de Investigaciones, el Servicio Secreto y el Departamento de Justicia). Pienso que también son muy importantes el Departamento de Comercio, el Departamento de Hacienda y el Departamento de Transporte. A todos ellos se les ha pedido que trabajen juntos en la creación de un plan nacional.

Lo que es más importante, sin embargo, se les ha pedido que trabajen en colaboración con el sector privado, debido a que prácticamente toda la llamada infraestructura esencial, vulnerable al ataque, pertenece, ciertamente, al sector privado. Si no contamos con la cooperación y el apoyo total del sector privado para desarrollar la capacidad de protegernos, no vamos a ir muy lejos.

P.: ¿En qué forma podrá medir el éxito de su misión?

HUNKER: Es difícil, porque es un problema nuevo y porque, de muchas maneras, los tipos de ataques y amenazas que el presidente nos ha pedido proteger a la nación, están en evolución, son realmente nuevos. En algunos casos no han surgido todavía y medir el éxito en este caso va a ser difícil. Creo que una importante medida del éxito va a ser el grado en que el sector privado (los propietarios y operadores de la red de energía eléctrica y nuestros sectores de transporte, banca y finanzas) se una para diseñar, junto con el gobierno, un plan de acción. Dentro de los próximos seis meses a un año podremos medir cómo se ha formado esa asociación. Esa es realmente la primera medida importante de éxito.

P.: ¿Qué plazos debe usted cumplir?

HUNKER: Es un plazo apremiante, porque la amenaza que preocupa al presidente (ataques electrónicos coordinados y complejos contra infraestructura esencial del país) existe actualmente. El presidente ha pedido para el año 2000 un plan nacional con la capacidad inicial de proteger de los nuevos tipos de ataques

cibernéticos. Y ha solicitado, para el año 2003, una capacidad de proteger la nación que esté en plena operación. La amenaza a que nos enfrentamos es del tipo que aumenta con el tiempo. De manera que tenemos que responder reconociendo la urgencia y llegar rápidamente a resultados reales para combatirla.

P.: Entiendo que usted piensa tener algo listo para noviembre.

HUNKER: Así es. En verdad, uno de los pasos realmente prioritarios requeridos por el presidente en su declaración en mayo pasado fue que dentro de seis meses, o sea a mediados de noviembre, los organismos del gobierno federal deberán haber progresado considerablemente en la preparación de sus propios planes para proteger la infraestructura esencial de que son responsables. Esto significa que, entre otras cosas, el Departamento de Hacienda y el Departamento de Defensa habrán creado un proceso para montar defensas que los protejan de ataques electrónicos. Segundo, el presidente nos pidió que tuviéramos dispuestos los elementos más importantes de un plan nacional más amplio que implicará una colaboración muy estrecha con el sector privado, integrar el trabajo que realizan varios organismos diferentes y obtener la participación de universidades, investigadores y demás. De manera que hay muchos elementos diversos. El plan nacional no habrá quedado establecido en noviembre, pero habremos dado pasos importantes hacia él.

P.: ¿Cómo evaluaría la naturaleza y gravedad de la amenaza a la infraestructura esencial de Estados Unidos y qué sectores son más vulnerables?

HUNKER: Para comprender la amenaza y vulnerabilidad de la infraestructura esencial de Estados Unidos debemos comenzar realmente por comprender la forma en que se ha desarrollado la economía. Durante el último par de años, debido al crecimiento de la Internet, cuyo uso y volumen se duplica cada diez meses, se ha producido la interconexión de todos los servicios vitales básicos de los que dependen los estadounidenses (como la energía eléctrica, nuestro sistema bancario, nuestro sistema de telecomunicaciones). Esos sistemas

constituyen la base del crecimiento económico y del apoyo a misiones vitales de seguridad nacional, y actualmente todos ellos son vulnerables.

A principios de este año tuvimos un ejemplo, durante la concentración militar que tuvo lugar a raíz de las actividades iraquíes. En ese entonces hubo pruebas de que intrusos cibernéticos habían entrado en computadoras del Departamento de Defensa que contenían información confidencial. Durante varias semanas ello preocupó a altas esferas del gobierno, mientras los técnicos examinaban el origen de la irrupción. ¿Provenía de Iraq o de sus aliados? Resultó que se trataba de un par de adolescentes estadounidenses, intrusos cibernéticos, que tenía la asesoría de alguien en el exterior. Pero eso da una idea del tipo de vulnerabilidad que encaramos.

Otro intruso cibernético, también adolescente, esta vez en Massachusetts, incapacitó una gran porción de la red telefónica de ese estado, con lo cual hizo que un importante aeropuerto quedara ciego electrónicamente durante un tiempo y hubiera una amenaza real a la seguridad del transporte aéreo. Si los intrusos, por sí solos, pueden causar ese tipo de daño, imagínese lo que podría hacer un ataque refinado y organizado encaminado a incapacitar sectores grandes de nuestro sistema de energía o nuestro sistema de telecomunicaciones o penetrar en información secreta. Esa es la naturaleza de la amenaza que encaramos. Y hay muchos indicios que indican que gente en otros países conoce y desarrolla este tipo de capacidad ofensiva para atacar a Estados Unidos electrónicamente.

P.: Como director de CIAO, usted coordina un programa nacional de información y concientización. ¿En qué consiste la información que quiere impartir y cómo la transmite a los ciudadanos de Estados Unidos?

HUNKER: Es importante que al hablar de información y concientización lo consideremos en dos mensajes diferentes. Uno se refiere a la concientización. Nos encontramos ante una nueva era y este es un nuevo tipo de amenaza que sólo recientemente ha llegado a ser objeto de gran atención. Por lo tanto, la concientización es obviamente parte de la información. Sin em-

bargo, me he sentido complacido porque (cuando hablo con el gobierno a nivel de gabinete y a niveles muy altos) la gente comprende la naturaleza de la amenaza. Los principales líderes empresariales y académicos ya lo entienden.

Nuestro segundo mensaje es ¿qué podemos hacer al respecto? Y por esa razón vamos a crear una asociación entre la industria privada y las diferentes partes del gobierno para lograr una acción real, en los meses venideros y, desde luego, en los próximos años, que responda a esto.

P.: ¿Cómo describiría usted el grado en que hemos llegado a depender de las computadoras, no sólo en la vida personal, sino para el funcionamiento básico de nuestra sociedad?

HUNKER: Mire alrededor suyo en su casa, mire en cualquier oficina donde trabaje. Lo que ve es nuestra dependencia de los sistemas electrónicos. Cuando vamos al banco y usamos el cajero automático, ése es un sistema electrónico que tiene conexiones nacionales e internacionales. Nuestra red de energía eléctrica la controla cada vez más, la Internet. El transporte aéreo y los ferrocarriles, todos dependen de sistemas electrónicos. Incluso las compañías que uno no considera que son compañías de computadoras o programas, dependen para sus operaciones y productividad de sistemas de información que están interconectados.

Se calcula que entre un tercio y una mitad del crecimiento económico que se ha visto en este país en el último par de años, período en que se han creado cientos de miles de empleos, proviene del comercio electrónico. Esa es la base de nuestro crecimiento económico en el futuro; es también la base sobre la que se apoya nuestra misión de seguridad nacional, bien se trate de la movilización de material y personal en cualquier parte del mundo, o de la obtención de información vital o de inteligencia sobre amenazas. Todo ello se basa, esencialmente, en estos nuevos sistemas electrónicos.

P.: ¿Cómo colabora usted con los sectores

privados comerciales e industriales para proteger mejor las redes de información y comunicaciones estadounidenses?

HUNKER: La estrecha colaboración con el sector privado es realmente fundamental para la meta y la misión que ha fijado el presidente. Puede no ser totalmente cierto, pero es bastante exacto decir que entre 90 y 95 por ciento del sistema de comunicaciones del Departamento de Defensa es realmente de propiedad privada y lo administra el sector privado. Es vital. A menos que involucremos al sector privado no iremos muy lejos.

Actualmente participo en una serie de reuniones con otros altos funcionarios del gobierno de diferentes departamentos, entre ellos el de Hacienda y el de Transporte, y con líderes del sector privado en industrias de la infraestructura fundamental como la banca y el transporte, por ejemplo, como parte del esfuerzo coordinado para establecer la asociación entre el gobierno y el sector privado.

El 1 de septiembre estuve en Charlotte, Carolina del Norte, en una reunión con el alcalde y otros funcionarios de la ciudad y el condado, así como con altos ejecutivos de algunos de los principales bancos. Charlotte es el segundo centro bancario del país. El propósito de mi visita era asegurarme de que los principales bancos de Charlotte formen parte de la asociación.

Tenemos planes en marcha para una serie de reuniones más adelante, este otoño, que incluirán al presidente, al vicepresidente y al asesor de seguridad nacional, así como a líderes de los sectores de energía eléctrica, la banca, finanzas, transporte y demás elementos de la infraestructura, con el objeto de afianzar realmente esta asociación.

Es un proceso largo. La creación de asociaciones, especialmente en un campo en que no hemos trabajado juntos antes, no es cosa que se haga de la noche a la mañana. Me he sentido muy complacido, sin embargo, con el tipo de reacción y conocimiento y colaboración real que he visto por parte de los gerentes generales, presidentes y altos ejecutivos de todas las industrias con las que he estado trabajando.

P.: ¿La CIAO está en contacto con la comunidad y los programas académicos para ayudar a encontrar mejores medios de asegurar la información y demás infraestructura vital de Estados Unidos?

HUNKER: La comunidad académica va a ser otra parte importante del tipo de asociación en la que estamos trabajando. De hecho, en septiembre, me reuní personalmente con los rectores y decanos de varias universidades principales (la Universidad de Carolina del Norte, Purdue University, el Instituto de Tecnología de Massachusetts, la Universidad de Virginia, para mencionar unas pocas). Y la razón para ello es realmente doble. En este momento, en este país tenemos una seria escasez de especialistas en computadoras y especialistas en informática. Y la amenaza de ataques cibernéticos simplemente va a aumentar la escasez que experimentamos. Va a aumentar la demanda de gente capacitada. Y van a ser las universidades las que estarán en la primera línea de la capacitación del tipo de gente que vamos a necesitar.

También vamos a necesitar el tipo de investigación y aplicación de los resultados que pueda encontrar nuevas soluciones, nuevas tecnologías para proteger nuestros sistemas de información. Y las universidades van a ser parte clave para ello.

P.: Como director de CIAO, usted tiene la responsabilidad de presentar iniciativas legislativas. ¿Cuál es su relación con el Congreso estadounidense y cómo evalúa la influencia de éste en las políticas y estrategias relacionadas con los objetivos de la CIAO?

HUNKER: El trabajo con el Congreso es una parte muy importante de este proyecto. Y yo diría que el interés parlamentario ha sido sumamente alto y el Congreso ha demostrado un gran apoyo a la búsqueda de una solución de esta nueva forma de terrorismo o amenaza a la seguridad nacional. Me imagino que habrán varias cuestiones importantes en las que continuaremos trabajando con el Congreso, ciertamente en lo que se refiere a recursos.

Como parte del trabajo que llevamos a cabo, creo que el presidente incluirá en su presupuesto del año fiscal 2000 una iniciativa importante para

proteger la infraestructura esencial. Esta incluirá recursos para investigación y desarrollo; recursos para nuevos programas de capacitación para especialistas en informática, tanto para el gobierno federal como para el sector privado y, quizá, otras iniciativas. De manera que el apoyo en cuanto a los recursos será muy importante.

El Congreso también examinará el conjunto de las leyes que ya existen sobre seguridad en la computarización. A menudo un intruso cibernético pasa a menudo por varias computadoras diferentes antes de llegar finalmente a la computadora donde realmente quiere realizar su incursión. Según la ley actual, si se quiere averiguar dónde ha estado ese manipulador y éste ha pasado por varios estados, es necesario obtener diferentes autos de registro domiciliario de jueces en todas partes del país, para poderlo hacer. Nos proponemos colaborar estrechamente con el Congreso en el examen de los procedimientos y protecciones legales que existen actualmente.

P.: ¿Percibe usted la necesidad de una mayor colaboración y cooperación internacionales para la protección de infraestructuras claves, y si es así, cómo podrían lograrse?

HUNKER: El aspecto internacional es algo que toca todo lo que se relaciona con el mundo cibernético. Estamos hablando de una amenaza que puede venir del extranjero; también puede venir del interior del país. Pero este tipo de amenaza no requiere necesariamente que la gente esté cerca de la institución o infraestructura que quiere atacar.

El año pasado se presentó una situación en la que un intruso cibernético de Alemania, que era en realidad un ciudadano de India, incursionó en un sistema financiero en Miami con el propósito de extorsionar. Así que en ese caso tenemos a dos países y a los ciudadanos de tres países involucrados en un incidente que atacaba directamente una institución estadounidense. Eso le da un pequeño ejemplo del aspecto internacional de todo esto.

La comisión presidencial sobre Protección de la Infraestructura Esencial emitió su informe el año pasado, luego de examinar este asunto durante

dos años. Sus recomendaciones fueron claves para el esquema anunciado por el presidente en mayo. El informe reconoció la gran importancia de la dimensión internacional.

El presidente encargó al Departamento de Estado tomar la iniciativa en nuestras discusiones con otros países en cuanto al intercambio de información y la posibilidad de nuevos tratados o protocolos para responder a ataques terroristas o de otra clase que puedan ocurrir. Ya varios países han expresado interés. Yo me he reunido con representantes del gobierno canadiense y del gobierno mexicano y sé que se han celebrado conversaciones dentro del contexto de la OTAN y de otras organizaciones internacionales sobre la materia.

De manera que hay un gran interés, pero estamos en una etapa muy inicial en cuanto a la forma en que evolucionará el aspecto internacional.

Otra cuestión importante es la superposición del trabajo para proteger de ataques cibernéticos, bien sea que provengan de delito organizado o de grupos de terroristas o de otros países, y lo que se ha llamado el problema de las computadoras en el año 2000 (Y2K). El Y2K es diferente porque sabemos exactamente cuándo ocurrirá el problema y es algo que cometimos nosotros mismos, porque hace años los programadores de computadoras no tuvieron en cuenta que el año 2000 tendría un conjunto de fechas diferentes del año 1900. (Muchos sistemas viejos de computadores usan solamente los dos últimos números del año para mantener las fechas actualizadas).

Sin embargo, de muchas formas la solución de la amenaza Y2K requiere exactamente el mismo conjunto de medidas que la protección contra ataques cibernéticos. Las instituciones, las compañías, el gobierno federal tienen que empezar por precisar el tipo de sistemas que tienen y la forma en que están interconectados, y luego decidir cuáles son los sistemas más importantes que proteger y la forma de hacerlo.

Otro aspecto del problema del año 2000 que se superpone a la amenaza de ataques cibernéticos es la creación de una capacidad que abarque

todo el país para responder o reconstruir los sistemas si algo anda mal cuando llegue el año 2000. Ese va a ser el modelo de una capacidad nacional para responder también a ataques cibernéticos. Involucrará industrias claves, organismos estatales y locales encargados de emergencias y partes claves del gobierno federal. De hecho, mi oficina colabora muy estrechamente con John Koskinen, asesor especial del presidente para cuestiones del año 2000, en varios aspectos de este proyecto de superposición del Y2K y cuestiones cibernéticas.

EL PROBLEMA DEL AÑO 2000

Por John Koskinen

Presidente del Consejo Presidencial para la Conversión del Año 2000

(El jefe de la iniciativa del gobierno de Estados Unidos para atender el problema de computadoras del año 2000 dice que el obstáculo principal que hay que superar es la “percepción insuficiente” del problema entre “los líderes gubernamentales, los periodistas, los ejecutivos de empresas y el público en general” de todo el mundo. Koskinen teme que la “falta de actividad y percepción pueda hacer que se materialicen algunos de los peores escenarios”. Pero recalca que “al emprender acción ahora podemos minimizar las perturbaciones y, es de esperar, efectuar una transición sin tropiezos al año 2000”).

El mundo enfrenta actualmente uno de los grandes retos de la Era de la Información. A medida en que nos encaminamos a un nuevo milenio, muchos sistemas de computación, así como los circuitos integrados que forman parte de prácticamente todo, desde las computadoras personales hasta los aparatos domésticos y el equipo industrial refinado, están destinados a retroceder en el tiempo.

El problema es que muchos sistemas más antiguos de computadoras y circuitos integrados utilizan sólo los dos primeros dígitos de un año para registrar la fecha. De esta manera, cuando llegue el año 2000, esos circuitos integrados pueden reconocer 00 como el año 1900, no 2000. El mal funcionamiento resultante ocasionaría graves alteraciones de los circuitos de energía eléctrica, plantas de tratamiento de agua, redes financieras, sistemas de telecomunicaciones y sistemas de control de tráfico aéreo en todo el mundo. En un mundo cada vez más interconectado dentro de una economía mundial, las redes de computación son tan fuertes como su vínculo más débil. Si bien cada nación posiblemente experimente sus propios problemas de sistemas en particular, en un sentido bastante real, estamos todos en esto.

¿Por qué los diseñadores de programas de computadoras cometerían un error tan obvio? Hace 30 años, la memoria de las computadoras era mucho menor que en la actualidad, por lo que los programadores recurrían a atajos, como indicar el año con dos dígitos, para ahorrar memoria. Asumían que los programas que

diseñaban pasarían de moda y serían reemplazados otros nuevos mucho antes del año 2000. Con todo, en la práctica, muchos sistemas de computación grandes y complicados, tales como los que emplea la banca, las aseguradoras o los corredores de bolsa han evolucionado con el paso del tiempo, añadiendo el último programa de computadora a los sistemas existentes. En consecuencia, cualquier organización que opera sistemas de computación interconectados a gran escala deberá revisar millones de líneas de código de computación para determinar cómo se manejan las fechas, acto seguido rescribir el programa para corregir el problema, luego poner a trabajar esas aplicaciones para ver cómo funcionan y posteriormente revisar la comunicación de cada programa con las aplicaciones internas y externas que utiliza.

No es difícil el ajuste tecnológico, pero debido a la gran escala de los problemas del año 2000, nos encontramos frente a un enorme desafío organizativo y gerencial. Sólo para citar un ejemplo: existe un grupo limitado de personas capacitadas para corregir el entuerto, programadores diestros en lenguajes de computación que pudieron haber quedado obsoletos hace años.

A fin de coordinar la labor en torno a este problema dentro de los muchos sistemas del gobierno estadounidense, el presidente Clinton ha formado un consejo de más de 30 agencias. Nuestra meta primordial consiste en mantener los servicios gubernamentales básicos: garantizar

que se sigan concediendo los beneficios relativos a la asistencia médica y el desempleo, que la recaudación de impuestos no se vea alterada. El objetivo ambicioso del presidente es que el 100 por ciento de los sistemas gubernamentales esté "de acuerdo con el año 2000", esto es, ajustado, para marzo de 1999. Asimismo, el consejo cuenta con grupos de trabajo dedicados a la intercomunicación con los gobiernos estatales y locales en torno a este problema y a la evaluación de los esfuerzos de las compañías privadas en 35 sectores industriales, tales como transporte, telecomunicaciones y finanzas.

Por otra parte, nos inquieta la situación en cuanto a los esfuerzos para resolver el problema del año 2000 en otros países, toda vez que muchos sistemas de computación cruzan las fronteras nacionales y en la economía mundial ninguna nación es una isla digital en sí. Estamos trabajando a través de agencias internacionales para abordar el problema. La Organización de las Naciones Unidas aprobó una resolución que exhorta a todos los estados miembros a emprender acciones y notificarlo a la Asamblea General para el 1 de octubre. El Banco Mundial celebra 20 conferencias regionales para incrementar la percepción pública de este tema, a lo que Estados Unidos contribuye con un aporte de 12 millones de dólares. El Fondo Monetario Internacional ha convenido en ejercer toda su influencia para alentar a los países a que inviertan recursos en el problema. La secretaria de Estado Madeleine Albright ha enviado un cable a las embajadas estadounidenses en todo el mundo, donde gira instrucciones a los embajadores para que indaguen en cada país anfitrión acerca de su grado de preparación para el año 2000. El Servicio Informativo y Cultural de Estados Unidos (USIS) encabeza un grupo de trabajo del Consejo Presidencial cuya misión es incrementar la percepción pública del problema, servir de puerta de acceso a la información y

concentrarse en un plan de contingencia con otros países.

Desafortunadamente, a estas alturas, cuando faltan menos de 500 días para el 1 de enero del año 2000, considero que el mayor problema sigue siendo el de la percepción del problema por parte de dirigentes gubernamentales, periodistas, empresarios y el público en general en muchos países. El primer paso es que las naciones y las empresas privadas hagan un inventario de todas sus operaciones que abarcan computadoras y desarrollen un plan para corregirlas. Un segundo paso de vital importancia es la planificación de contingencia. El Consejo Presidencial para el Año 2000 ha solicitado a cada agencia gubernamental estadounidense que elabore dos tipos de planes: uno, ¿qué haremos si algunos de nuestros sistemas de computación no funcionan? El segundo nivel comprende un plan de contingencia externo: ¿qué haremos si fallan los sistemas interconectados con los nuestros?

Es posible que las perturbaciones relativas al año 2000 comiencen antes del nuevo milenio en la medida en que los sistemas anacrónicos intenten calcular o programar acontecimientos futuros. Es difícil predecir en este momento qué pasará precisamente. Existe un cúmulo de sitios en laWeb en Estados Unidos donde algunos expertos a los que nadie catalogaría de alarmistas han pronosticado fallas extendidas del sistema que conducirán a interrupciones de energía eléctrica, problemas de tránsito, recesión económica y, posiblemente, en ciertas regiones, déficit de alimentos. Aunque tiendo a ser más optimista que estos profetas del desastre, me preocupan particularmente los países donde la inactividad y el desconocimiento podrían llevar a la materialización de algunos casos extremos. El caso es que al emprender acción ahora podemos reducir al mínimo las perturbaciones y, es de esperar, efectuar una transición ininterrumpida al año 2000.

LA AMENAZA DE LA GUERRA INFORMATICA REQUIERE MAYOR ATENCION EN TODOS LOS FRENTE

Entrevista con el senador Jon Kyl

(Ni la administración, ni el Congreso, ni el público en general dedican la debida y suficiente atención a la creciente amenaza de una guerra informática (o guerra I), dice el senador Jon Kyl. Nuestros adversarios potenciales perfeccionan su capacidad de atacar las infraestructuras esenciales que cada vez más corren a cargo de las comunicaciones, el transporte y los sistemas financieros de nuestro país, así como de su vital sistema de defensa, advierte el senador. Kyl, republicano por Arizona, dirige la Subcomisión de Tecnología, Terrorismo y Estado de la Comisión de lo Judicial del Senado. Es también miembro de la Comisión del Senado sobre Asuntos de Inteligencia. Kyl fue entrevistado por el redactor colaborador Ralph Dannheisser.)

PREGUNTA: En una audiencia de la comisión, el pasado junio, expresó usted que la “parte digital, la más débil y sensible” de Estados Unidos es más vulnerable a ataques que las fuerzas militares de la nación. ¿Puede ampliar un poco ese tema?

Creo que es algo que ya todos aceptan como cierto. Contamos con una fuerza militar insuperable en el mundo y nadie tiene la capacidad de retornos. De modo que la pregunta que nos debemos plantear es si un posible adversario quisiera atacar los puntos más débiles de nuestra infraestructura informática, ¿podría intentarlo? Lo mismo nos tenemos que preguntar sobre los terroristas. La respuesta es que nuestra infraestructura informática es uno de nuestros puntos vulnerables porque, más que ninguna otra nación, dependemos de la tecnología avanzada en nuestras comunicaciones, nuestro transporte, nuestras operaciones financieras e incluso, claro está, en nuestro sistema de defensa. Como consecuencia de ello, la vulnerabilidad de nuestra infraestructura informática sería, probablemente, el blanco clave de un estado agresor o de una organización terrorista.

P: Sobre ese mismo tema ha mencionado usted que se trata de la cuestión más difícil e importante de seguridad nacional, y la más preocupante para la seguridad pública, que el liderazgo de nuestro país tendrá que afrontar en

los próximos años. ¿Cuáles son algunos de sus mayores temores si no se le presta la debida atención a esta cuestión?

KYL: Tomemos como punto de partida la transición al nuevo milenio. El problema informático del Año 2000, que correctamente ha sido identificado como el problema en potencia más serio para el país, se ve agravado por el mero hecho de que presentará a terroristas y a otros grupos o particulares que interesan perjudicarnos con una oportunidad inigualable para atacarnos en momentos de mucha confusión. No sabremos por qué marcharán mal las muchas cosas que marcharán mal cuando toque la medianoche del 31 de diciembre de 1999. Es probable que atribuyamos la mayoría de los problemas a las fallas del Año 2000 en las computadoras, pero es obvio que presenta una gran oportunidad para realizar sabotajes u otros ataques a nuestra infraestructura por los que quieren perjudicarnos — tanto porque sus actividades quedarán veladas bajo el manto del acontecimiento en curso, como también por la vulnerabilidad que entraña el propio acontecimiento.

De modo que ahí ya se tiene la primera gran oportunidad, pero aparte de este momento en el tiempo — por lo que he dicho de la vulnerabilidad de los diferentes aspectos de nuestra sociedad

civil y de ciertos componentes de nuestra defensa — el ataque a nuestra infraestructura viene a ser una de las mejores formas de perjudicarnos en lo abstracto y, en una situación de conflicto permanente, representa una gran oportunidad para causar trastornos a nuestra capacidad de afrontar las amenazas que surjan de una situación imprevista.

P: En general, ¿cuán fácil es infiltrar el sistema informático en determinado momento y qué tipo de daños puede ocasionar alguien que tenga éxito en su intento?

KYL: Pues bien, es sorprendentemente fácil. Es difícil cuantificarlo en palabras, pero recientemente se han llevado a cabo algunos ejercicios. Uno que ha ocupado titulares en los medios informativos es el llamado “Receptor elegible”, que ha demostrado en términos reales cuán vulnerables son el sistema de transporte, el de energía eléctrica y otros a los ataques de intrusos cibernéticos, personas que utilizan equipo común y corriente, nada de equipo de espías. Sólo con lo que hay disponible se pueden perturbar aspectos claves de nuestra infraestructura informática. Ahora bien, en el ejercicio al que me he referido, se han perturbado partes del sistema financiero, el de energía eléctrica y el de transporte. Otros que son vulnerables son los sistemas de acueductos, todas las formas de telecomunicaciones, claro está, y el personal de los servicios de respuesta inmediata, pero quizá desde el punto de vista de la defensa no hay nada más serio que los laboratorios del sistema de defensa y los sistemas de armamentos.

De modo que el grado de vulnerabilidad es alto y cada vez que unos de estos jóvenes intrusos cibernéticos de otros países se introducen en el sistema de computadoras del Pentágono, la gente se pregunta cómo puede haber sucedido y qué puede aprenderse del incidente. Y parece que es ahora un proceso continuo de aprendizaje. Otro ejemplo: antes del incidente iraquí del pasado febrero, cuando estuvimos a punto de invadir y hacerle algo a Saddam Hussein, la intervención de los intrusos cibernéticos en las computadoras del Pentágono fue tan significativa que se le advirtió al presidente que la actividad podía ser resultado de una acción intencional del gobierno iraquí. Hubo momentos en los que no sabíamos si ello era la causa o no. Resultó que

eran tres jóvenes de tres países diferentes. De modo que para responder a su pregunta de cuán vulnerables somos, creo que este ejemplo viene muy bien al caso.

P: Ciertamente que el hecho de que estos jóvenes a quienes no impulsan motivos siniestros puedan introducirse tan fácilmente en los sistemas informáticos nos revela que nuestros adversarios pueden hacer lo mismo con mayor posibilidad de daño.

KYL: Esa es precisamente nuestra preocupación.

P: Desde su punto de vista como miembro de la comisión y con su sobrado interés en el tema, ¿cuál cree usted que será la función del Congreso en la protección contra este tipo de guerra informática o de terrorismo cibernético?

KYL: Pues bien, lo obvio — tenemos que dar dinero suficiente a los organismos de seguridad nacional y a la maquinaria militar, y la autoridad para afrontar el problema.

Todo ello supone cuestiones muy reales, pero creo que desde el punto de vista de política pública lo principal es establecer la política del gobierno, tomarla muy en serio y proporcionar los medios para llevarla a cabo.

Hemos estado impulsando a la administración del presidente Clinton durante cuatro años, pero todavía no hemos logrado lo que queremos. Se suponía que presentarían un plan y todavía no se ha logrado. Lo que el presidente hizo mediante una orden ejecutiva fue exigir se elaborara un plan en el plazo de 180 días. Así que ahora estamos en compás de espera. El 22 de noviembre es la fecha límite. Así que, probablemente, ese sea el plan que los organismos gubernamentales utilicen para afrontar este problema.

P: ¿Esto ha sucedido a instigación del Congreso?

KYL: El Congreso puso el proceso en marcha al solicitar dos veces o requerirle dos veces al presidente que presentara un plan o informe. No lo hizo. Lo que hizo fue, primero, nombrar a una comisión y, luego, nombrar también a un grupo de estudio de funcionarios de gobierno que forma parte de esa comisión. Entre las

recomendaciones que hicieron figuraba la elaboración del plan del que antes hablábamos. Así que, durante mucho tiempo, han estado proyectando dar inicio a los informes y ahora estamos llegando al final de ese proceso de 180 días. Tengo la esperanza de que el plan proporcione, como mínimo, las directrices que debe seguir cada organismo clave del gobierno en su relación con el sector privado para proporcionar orientación, por lo menos, en una primera etapa de actividad. Pero le falta todavía la parte significativa del componente de defensa, que creo debe ser la próxima en la que la administración debe concentrar su atención. Así que creo que nuestra función es seguir instigando y proporcionando los recursos que sean necesarios.

P: ¿Le parece que la cuestión está recibiendo de los legisladores la atención que requiere ese objetivo?

KYL: No, pero tampoco ha habido desacuerdo en la rama legislativa. Ha sido un esfuerzo bipartidista y bicameral. De modo que ese no es el problema, pero si me pregunta si el Congreso o el público en general tiene la suficiente comprensión de este tema, la respuesta es no. Y tampoco hay la comprensión o el compromiso de parte de la administración.

P: Usted ha hablado indirectamente de ello, pero dada la interconexión de la infraestructura informática, ¿es necesario que el sector privado y el sector público coordinen de alguna manera sus actividades sobre este asunto y trabajen unidos?

KYL: Sí, y parte del plan que prevemos que la administración elaborará abordará el elemento de coordinación. Por ejemplo, el Departamento del Transporte tendrá, probablemente, un plan para integrar los componentes de la industria privada del transporte y el Departamento del Transporte en una respuesta conjunta —indicaciones, advertencias y respuestas, y así sucesivamente. Hay también un grupo industrial experto en el área de telecomunicaciones con el que el presidente viene laborando desde hace algún tiempo. Este grupo sigue proporcionando asesoramiento sobre los requerimientos del sector privado y sobre qué se puede hacer para atender esta situación. Porque, por último, es el equipo y la tecnología generada por el sector privado los que son utilizados tanto por el sector

privado como por el gobierno, y pueden ser muy innovadores en lo que integran en los sistemas y las soluciones que proporcionan al gobierno. Es lo que han estado haciendo.

Q: Mencionó usted antes la sospecha, que luego resultó ser que no era cierta, de que en determinado momento se pensó que Irak tomaba parte en alguna actividad de guerra informática. ¿Sabe usted de algún adversario de Estados Unidos que esté activamente haciendo estos preparativos y de qué tipo son?

KYL: Según nuestros servicios de inteligencia, hay un gran número de países que trabajan en técnicas de guerra informática y hay otro número reducido de países que tienen a Estados Unidos como blanco específico en la elaboración de sus planes. No puedo decir si ha habido alguna vez un intento de atacar nuestra infraestructura informática por otro país.

P: Imagino que los ataques podrían suceder de una de dos maneras, o bien con la cesación de algunas actividades controladas por el sistema informático o bien mediante la introducción de información falsa en los sistemas informáticos.

KYL: Se puede entrar y sacar información, se puede introducir un defecto o error en un programa para interrumpir o detener las operaciones, o se puede introducir información falsa. De modo que se pueden hacer todas las tres cosas.

P: Y, es probable que alguien en alguna parte esté ahora considerando este tipo de intento.

KYL: Como he dicho antes, hay un gran número de países con programas en curso, algunos de los cuales tienen como blanco a Estados Unidos. Ahora bien, hay que hacer la salvedad de que no quiero decir con eso que hay países que intentan atacar hoy a Estados Unidos. Sencillamente digo que ya se han desarrollado programas o que se está en proceso de trabajar en el concepto de una guerra informática contra Estados Unidos. Me parece lógico y puede que su próxima pregunta sea si Estados Unidos debe pensar en tomar la ofensiva o actuar a la defensiva.

P: ¿Puede elaborar un poco?

KYL: Lo único que agregaría es recordar a los lectores con respecto a la capacidad de emprender una ofensiva en la guerra informática es que somos, por mucho, el país más vulnerable debido a nuestro grado de dependencia de la tecnología, de modo que para nosotros se trata más de actuar a la defensiva que tomar la ofensiva.

P: Pero ha insinuado usted que ciertamente que se están haciendo preparativos o investigaciones aquí también.

KYL: Recuerde que, poco después de la operación Tormenta del Desierto, se difundió información que revelaba el grado en que Estados Unidos trastornó las comunicaciones iraquíes y sobre otras actividades que se puede decir son un primer ejemplo de una guerra informática. En realidad no se trata de algo nuevo. Quiero decir que, durante años, hemos intentado intervenir en

las comunicaciones del enemigo y descifrar su codificación. Ahora se trata de una versión de lo mismo con una tecnología más avanzada.

P: ¿Qué proyecta hacer en este momento en la subcomisión con respecto a otras actividades?

KYL: Lo próximo que haremos será hacer examen del informe que se emita en noviembre en respuesta a la Directiva Presidencial, que será el que nos dé una indicación de lo que la administración proyecta hacer, para luego evaluarla y quizá celebrar audiencias para conocer sus intenciones y escuchar opiniones de otras personas, y no estoy seguro en este momento de lo que haremos después.

P: ¿PREVEE usted que, en algún momento, habrá que asignar un monto considerable de fondos?

KYL: En realidad bastante pocos, pero diría que sí habrán requerimientos de financiación.

¿FANTASMAS EN LAS MAQUINAS?

**Por el doctor Martin Libicki
Analista de políticas principal, RAND**

(El autor cita las actividades policiales como un área primaria en la cual se puede mejorar la seguridad de información mundial. Propone “la armonización de las leyes nacionales contra los ataques cibernéticos, cooperación multinacional para rastrear ataques a través de las fronteras nacionales, tratados internacionales de extradición de atacantes, y disposición a imponer sanciones a quienes protejan a los atacantes”. Cree que la disposición a compartir información sobre investigación y desarrollo acerca de indicaciones y advertencias de ataques, y sobre incidentes y respuestas a ataques, “también puede mejorar la eficacia de las medidas de protección de cada nación”).

Nadie que esté buscando un nuevo motivo de preocupación necesita ir muy lejos. En todas partes, las computadoras y los artefactos digitales se han instalado en nuestras vidas. Lo que antes era manual, ahora es automático; lo que era analógico ahora es digital; y lo que antes estaba solo ahora está conectado a todo lo demás. De modo creciente, no tenemos otro remedio que confiar en ellos. Si fallan, nos hundimos.

La confianza engendrada por la dependencia se justificaría si esos artefactos sólo hiciera lo que se suponen que deben hacer. Algunos fallan por sí solos, y seguimos adelante. Pero también existe la perspectiva de que puedan fallar porque han caído bajo el control de gente con intenciones malignas. En esas circunstancias, no sólo podrían fallar, sino también revelar secretos que se les han confiado, o producir información corrupta, algunas veces de maneras que no se perciben hasta que es demasiado tarde para revertir las acciones que ya se han puesto en marcha.

¿Por qué la vulnerabilidad? Los artefactos digitales son rápidos, baratos, precisos y raramente olvidan lo que se les dice. Pero también son terriblemente literales y generalmente carecen del discernimiento para comprender las implicaciones de lo que se les pide que hagan o la integridad de quienes les piden que lo hagan.

Las consecuencias potenciales de inducir deliberadamente fallas o corrupción de sistemas son vastas. Al tomar el control de sistemas clave que sostienen la estructura de la sociedad, los atacantes de computadora pueden, en teoría, oír llamadas telefónicas, desviar conexiones y paralizar completamente el servicio telefónico; cortar el suministro de energía eléctrica; infiltrarse en la manera en que literalmente millones de millones de dólares cambian de manos cada semana; obstaculizar los servicios de emergencia; impedir que las fuerzas armadas estadounidenses respondan rápidamente a crisis en el exterior; revelar secretos médicos personales; trastornar los sistemas de transporte y poner en peligro a los viajeros, y mucho más. La vida como la conocemos podría paralizarse.

Los ataques computarizados, si se los efectúa de manera suficientemente sistemática, podrían ser guerra por otros medios, y de allí viene el concepto amplio de “guerra de información”. Pero la guerra de información comprendida en términos amplios —atacar los procesos de información y de decisión de un adversario— es tan antigua como la guerra misma. Esas tácticas abarcan operaciones psicológicas, ataques contra el aparato de comando del enemigo, espionaje y contraespionaje, y operaciones contra las infraestructuras y sistemas de vigilancia adversarios. Durante la guerra civil estadounidense (1861-1865) hubo incidentes de operaciones de propaganda, francotiradores que atacaban a generales del bando contrario y

observadores en globos aerostáticos, incursores que desmantelaban líneas de telégrafo, piquetes de caballería y manifestaciones contra la caballería, todo ello parte de la guerra de información. Durante la segunda guerra mundial ocurrió el advenimiento de la guerra electrónica mediante el radar, el engaño electrónico, la interferencia de frecuencias de radio, la codificación de mensajes y el descifrado de códigos con ayuda de computadoras.

Los ataques computarizados se incorporan sin dificultad a este continuo de la guerra. Si uno puede destruir cuarteles generales enemigos con bombas y cañonazos, ¿qué está mal en usar medios menos violentos para penetrar y destruir los sistemas de computadoras que manejan las batallas del futuro? Las nociones de guerra estratégica de 1920 sostenían que el uso del poder aéreo contra blancos civiles reduciría la crueldad de la guerra de trincheras. La guerra de información estratégica es todavía mejor.

¿Son vulnerables las sociedades modernas? La mayoría de los sistemas de información tienen mucho menos seguridad de la que podrían tener; muchos de ellos, menos de la que deberían tener. Se han atacado redes y sistemas de muchos tipos: servicios de Internet, servicios telefónicos, algunos servicios de transporte, instituciones financieras y redes empresariales.

Los ataques computarizados, bajo cualquier definición, son un problema grave. En efecto, el Departamento Federal de Investigaciones estimó que le cuestan a la economía estadounidense entre 500 millones y 5.000 millones de dólares por año, cálculo que tiene un margen de error amplio y, de alguna manera, es muy revelador. Nadie sabe verdaderamente cuántos ataques ocurren. Muchas de las pruebas son anecdóticas, y la gente tiene que hacer conjeturas usando preceptos populares como "sólo los aficionados dejan impresiones digitales, los profesionales nunca lo hacen" y "nadie quiere hablar nunca de cuán duro lo han golpeado". De manera que a los ataques computarizados se los compara con témpanos, y supuestamente Estados Unidos desempeña el papel del Titanic.

Esta es la teoría, de cualquier manera. ¿Y cuál es la perspectiva? A diferencia de virtualmente todas las otras formas de guerra, no hay entradas forzadas en el espacio cibernético. Si los

intrusos cibernéticos entran en un sistema lo hacen invariablemente a través de caminos instalados en el propio sistema: algunos son pasajes y otros son problemas (es decir, pasajes indocumentados) que nunca se eliminaron. De cualquier manera, viajar por estos caminos está bajo el control completo de quienquiera que opera el sistema. Al ser así, la vigilancia debería ser protección suficiente.

En efecto, la protección existe. Muchos sistemas de información operan con varias capas: estas son maneras de separar los usuarios ilegítimos de los legítimos; cerraduras para impedir que usuarios legítimos tomen control deliberada o inadvertidamente de los sistemas de computadoras, y dispositivos de seguridad para que incluso la usurpación del control no cree un peligro público.

Los intrusos cibernéticos, por su parte, primero deben engañar al sistema haciéndole creer que son usuarios legítimos (robando o adivinando una contraseña), y segundo, adquiriendo privilegios de control (con frecuencia explotando fallas endémicas) negados a la mayoría de los usuarios comunes. Con esos privilegios de "super usuario", los atacantes pueden eliminar archivos claves, escribir disparates en otros, o abrir una puerta oculta para volver a entrar después.

También hay pocas dudas de que las defensas, si hiciera falta, podrían ser mejores que la práctica común de la actualidad.

La mayor parte de los sistemas usan contraseñas para limitar la entrada, pero las contraseñas tienen muchos problemas bien conocidos: demasiadas de ellas son fáciles de adivinar; pueden ser robadas al pasar por las redes, y generalmente se las guarda en lugares esperados de una computadora servidora o anfitriona. Los métodos criptográficos como las firmas digitales eliminan estos problemas (haciendo inservible capturar y repetir los mensajes de acceso). Las firmas digitales incluso ayudan a asegurar que todo cambio en un banco de datos o programa, una vez firmado electrónicamente, pueda ser rastreado a su originador, lo cual también es útil para el caso en que el atacante sea alguien de la propia firma que tiene privilegios de usuario.

Los sistemas operativos de las computadoras y redes son vulnerables a los programas insertados por intrusos cibernéticos, como los virus (programas de computadoras que infectan a otros programas y hacen que a su vez infecten a otros programas más); caballos de Troya (programas de computadoras aparentemente útiles con trampas ocultas) y bombas lógicas (programas que permanecen letárgicos hasta que se los despierta). La protección contra los virus podría dar resultado, pero si la preocupación persiste, ¿por qué no poner todos los archivos críticos en un medio inalterable (como un CD-ROM)? Semejante medio puede también impedir que la información sea borrada o corrompida por los rastros digitales de un atacante potencial. En efecto, dado el bajo costo de esos artefactos, ya no hay más excusas legítimas para perder información.

Los sistemas también pueden ser puestos en peligro desde otros sistemas que ellos consideran de confianza. Se pueden tomar dos precauciones contra este peligro: reducir la lista de sistemas de confianza y limitar la cantidad de mensajes a los que reaccionará el sistema propio. Por ejemplo, los sistemas bancarios hacen esto para proteger a sus computadoras de que las corrompan ATM (cajeros bancarios automáticos) instalados en la calle. La computadora hace caso omiso de todo mensaje de un ATM que no sea una transacción legítima. Ninguna transacción legítima puede destruir la computadora del banco.

Y una precaución final es desenchufarla. Como último recurso, muchos sistemas (como las plantas generadoras de energía nuclear) funcionan casi tan bien aunque no estén conectadas al mundo exterior.

¿Hasta dónde han de tomar medidas los que tienen computadoras? Puede que hoy día baste un garantizador de seguridad de costo relativamente bajo (v.g., cortafuegos y detectores de intrusos). Después de todo, es muy probable que no valga la pena invertir grandes cantidades de dinero en un sistema de oficina sólo para protegerlo ya que, por ejemplo, en caso de ataque, el servicio sólo se interrumpiría temporalmente. Hay muchas compañías que no se percatan del peligro y actúan en

consecuencia. Puede que tengan razón... pero, ¿y si están equivocadas? A medida que aumenta el peligro, los propietarios de los sistemas computarizados pueden añadir medidas de seguridad — incluso a corto plazo (v.g, pueden evitar que los usuarios accedan al sistema desde sus casas, o hacer que pulsen ciertos códigos para acceder al sistema).

Desde luego, es precisamente la falta de buenos dispositivos de seguridad en toda la infraestructura nacional de información de hoy, la que tiende en cierta medida a hacernos confiar en que, si fuera necesario, se podría garantizar la seguridad de los sistemas informáticos. (En contraste, una buena defensa en caso de una guerra nuclear fue durante décadas, algo imposible de lograr desde el punto de vista tecnológico y, aunque hoy sea posible, es sumamente costoso). Incluso aunque muchos sistemas computarizados queden inservibles temporalmente, es otra cuestión el mantenerlos inutilizados durante bastante tiempo mientras que los administradores de sistemas trabajan arduamente para restaurar los servicios esenciales. Cualquiera que amenace la infraestructura de información de Estados Unidos debe darse cuenta de que la mera amenaza — si se toma en serio — empieza a tener su efecto negativo tan sólo al poco tiempo de saberse públicamente, ya que la gente reacciona.

¿Cuál debe ser la función del gobierno? ¿Están capacitados los que protegen a la nación por tierra, mar y aire y en el espacio, para hacerlo también en el espacio cibernético? ¿Deberían hacerlo?

El gobierno puede ayudar, pero hay mucho que el gobierno no puede ni debe hacer. Por supuesto que la electricidad es esencial, pero proteger el suministro de electricidad del ataque de los intrusos cibernéticos depende casi totalmente de cómo las compañías eléctricas administran sus sistemas computarizados: con esto se entiende los programas que las compañías compran para la red y el sistema operativo, el número de programas que configuran para sus sistemas, cómo otorgan y protegen los privilegios de acceso y cómo los diferentes mecanismos de control manual y de funcionamiento se incluyen en todos los sistemas de generación y

distribución de la compañía. Es inconcebible que una compañía eléctrica esté dispuesta a que el gobierno la “proteja” y establezca las directrices para hacer estas cosas. En general, el gobierno no puede montar un cortafuegos alrededor de todo Estados Unidos — aunque sólo sea por el hecho de que hay tantas redes nacionales que se ramifican por todo el mundo.

El gobierno puede aplicar, y de hecho aplica, leyes que penalizan los ataques a los sistemas computarizados — y ha tenido bastante éxito si se tiene en cuenta el anonimato (y distancia) de que gozan los intrusos. Hasta la fecha, casi todos los más famosos ataques de intrusos detectados han sido obra de aficionados y no de profesionales.

¿Debería el gobierno intentar impedir la guerra informática y tomar medidas de represalia contra los malhechores? Supóngase que se pueda identificar quiénes son los autores. El gobierno de Estados Unidos tiene la capacidad de tomar represalias, pero hay muchos estados brutales que carecen sistemas comparables (v.g., Corea del Norte no tiene un mercado de valores que pueda ser inhabilitado). En el mismo orden de cosas, es un problema responder de modo violento contra un ataque informático que ha ocasionado pérdidas de tiempo y dinero, pero que no ha herido a nadie.

Aunque mucho de lo que el gobierno puede hacer para incrementar la seguridad es de modo indirecto, la Comisión Presidencial sobre la Protección de la Infraestructura Crítica y otras entidades han propuesto las siguientes recomendaciones:

— Cerciorarse de que los sistemas que el gobierno posee estén protegidos, porque son importantes para la seguridad nacional y como modelo estándar.

— Usar la investigación, el desarrollo y la adquisición primaria para promover el desarrollo rápido de instrumentos de seguridad.

— Divulgar avisos de alerta en casos de ataques evidentes de guerra informática, (si se pueden detectar, lo cual no es fácil).

— Promover un ámbito legal que conduzca al sector privado a proteger sus sistemas al máximo.

— Proveer un centro neutral de intercambio de información que ayude al sector privado a colaborar por medio de un intercambio, a nivel confidencial, de información sobre experiencias y medidas preventivas adoptadas.

Por lo general, tales medidas van progresando.

Por desgracia, las restricciones — existentes y potenciales — que el gobierno de Estados Unidos establece en torno al cifrado de alto nivel, han inhabilitado uno de los mejores medios de protección de sistemas y también han debilitado la confianza en las medidas adoptadas por el gobierno en torno a la guerra informática.

Actividades internacionales: extender la mayoría de estas medidas gubernamentales al extranjero indica una agenda abierta para guiar las actividades internacionales contra la guerra informática.

El campo de la aplicación de la ley es muy amplio. La armonización de las leyes nacionales que tienen que ver con la agresión informática, la cooperación multinacional en el rastreo de ataques que sobrepasan las fronteras nacionales, los tratados internacionales sobre la extradición de los intrusos y el estar dispuesto a imponer sanciones a aquellos que protegen a los intrusos, todo esto puede contribuir a la seguridad de la información en todo el mundo.

El estar dispuesto a compartir información sobre la investigación y desarrollo, sobre señales y avisos de ataques, así como sobre incidentes habidos y respuestas tomadas frente al ataque puede mejorar la eficacia de las medidas de protección de cada país. Sin embargo, estas áreas suelen ser ámbito exclusivo de las agencias de inteligencia, las cuales no se caracterizan por su transparencia en tales asuntos.

Conclusiones y pronósticos: en el mundo posterior a la Guerra Fría hay un aumento de peligros nuevos y no convencionales (v.g,

terroristas con armas nucleares) los cuales atemorizan, pero, por el momento, son sólo imaginarios. La guerra de la informática es uno de ellos. Cuantos más sistemas de información permeen la sociedad — sus defensas, comercio, vida diaria — más importante será para nosotros que funcionen bien. La posibilidad de graves daños es real, especialmente si los ataques son sistemáticos y los lleva a cabo un adversario bien financiado. Pero lo que también sorprende es el hecho de que aunque la guerra informática es relativamente barata, hasta la fecha casi no ha habido incidentes realmente graves.

Dos son los indicadores que nos pueden dar una idea clara del verdadero riesgo que se corre de sufrir un ataque cibernético. Uno es cómo reacciona la gente ante el problema de las computadoras del año 2000. Dése por supuesto que gran cantidad de los sistemas computarizados del mundo fallarán a medianoche del 31 de diciembre de 1999. ¿Cundirá el pánico

y se paralizará todo? o ¿hallará la gente el modo de solucionar el problema y prescindirá de la información durante un tiempo? Si empiezan a proliferar los pleitos, ¿qué precedentes se establecerán que asignen responsabilidad a individuos por el daño ocasionado, si los sistemas fallan?

El otro pronóstico es de origen más reciente. Si uno pudiera imaginar quién sería capaz de llevar a cabo ataques graves de guerra informática, pensaría en alguien que no tuviera nada que perder (v.g., no un país), que tuviera ocultos varios millones de dólares en efectivo, un cierto conocimiento tecnológico, una red internacional de amigos infames, un rencor contra Estados Unidos u otra nación por algo real o imaginado. ¿Les recuerda a algo? Si así es, el próximo año puede que se descubra la existencia de individuos o de grupos poderosos que intentan doblegar a algún país por medio de la guerra informática o, por el contrario, que éstos se concentran en otra cosa.

LA RESPUESTA DE LA EDUCACION SUPERIOR A LA GUERRA DE LA INFORMACION

Por el doctor Charles W. Reynolds
Director del Departamento de Informática y Decano Interino del Colegio de Ciencias y Tecnología Integradas, de la Universidad James Madison

(El doctor Charles Reynolds afirma que existe una creciente demanda de profesionales de la seguridad de la información en una era en que “el vandalismo criminal, la actividad criminal y la guerra internacional de la información” pueden poner en peligro la infraestructura nacional de la información. Describe la colaboración de la comunidad académica con el estado y la industria para atender a esa necesidad mediante un plan que se puso en marcha en 1997, al que se conoce por el título de Coloquio Nacional para la Educación en la Seguridad de los Sistemas de Información (NCISSE). El autor, presidente del comité ejecutivo del NCISSE en 1998, también hace una reseña breve de la labor que lleva a cabo la Universidad James Madison en respuesta a las nuevas prioridades nacionales para neutralizar las amenazas a las redes de información de Estados Unidos).

La necesidad de proteger la infraestructura de la información y las comunicaciones

Todos los aspectos de nuestra vida y de nuestros sistemas social, económico y político dependen cada vez más de nuestra infraestructura de información y comunicaciones. Nuestros sistemas financiero y de transportes, nuestros servicios públicos de agua y electricidad y todas las demás infraestructuras básicas dependen de nuestra infraestructura de información y comunicaciones. Sin embargo, ésta es la más vulnerable de todas nuestras infraestructuras al vandalismo criminal, la actividad criminal y la guerra internacional de la información, todos los cuales pueden amenazarla, así como a todas las demás infraestructuras que dependen de ella. La seguridad y garantía de nuestra infraestructura de información y comunicaciones es, por tanto, una prioridad nacional.

Para hacer frente a las amenazas de la nueva era de la tecnología de la información, nuestro país necesita una fuerza laboral educada en materia de información y consciente de las vulnerabilidades incipientes de las infraestructuras básicas, así como un plantel de profesionales de seguridad de la información con experiencia en las “prácticas óptimas” reconocidas en seguridad y garantía de la información.

Diálogo nacional con la educación superior

En mayo de 1997, en respuesta a la necesidad de proteger las infraestructuras críticas de la nación, se creó el Coloquio Nacional para la Educación en Seguridad de los Sistemas de Información (NCISSE) con el fin de establecer un foro para el diálogo entre figuras clave del gobierno, la industria y el mundo académico sobre posibles formas de asociación, con el propósito de definir las necesidades actuales y en surgimiento en materia de educación en seguridad de la información. El NCISSE también trata de influir en los programas de estudio de seguridad de la información e impulsar su elaboración y expansión, sobre todo en los niveles universitario y posgraduado.

En su segunda reunión celebrada en junio de 1998, en la Universidad de James Madison, en Harrisburg, Virginia, el Coloquio acordó desplegar sus mejores esfuerzos para fomentar la elaboración de programas de estudio que reconozcan la necesidad expresada por el gobierno y la industria y se basen en las “prácticas óptimas” existentes en el sector.

Los objetivos del Coloquio también están condicionados por la necesidad de ayudar a las instituciones docentes a fomentar la elaboración y el intercambio continuos de recursos de

educación en seguridad de la información. El NCISSE alienta a las instituciones docentes a enseñar cursos apropiados sobre seguridad de los sistemas de información en varios programas de estudios para atender a las necesidades de los consumidores del siglo XXI y ofrecer cursos para atender la creciente demanda de profesionales de seguridad de los sistemas de información.

En su reunión anual de 1998, el NCISSE hizo público un vasto programa de acción para las diversas entidades directamente interesadas en la seguridad de la información. Este programa incluía tareas que el gobierno, la industria y las instituciones de enseñanza superior realizarían individualmente y en cooperación entre ellos.

Una de esas actividades conjuntas que reviste especial importancia es la aclaración del conocimiento, las aptitudes y actitudes que definen al profesional de la seguridad de la información y la elaboración de normas sobre lo que debe saber y ser capaz de hacer. Dado que la información misma todavía no es una disciplina autónoma, necesitamos identificar las "prácticas óptimas" actuales para su inclusión en las normas profesionales, de modo que puedan seguir evolucionando. Por último, los tres integrantes del Coloquio deben superar la resistencia del personal de seguridad de la información a las normas, porque lo que se espera de cualquier profesión es su adhesión a la disciplina incorporada en un conjunto de normas.

En su esbozo de las actividades recomendadas para la industria privada, el Coloquio dice que el sector industrial debe facilitar a las instituciones docentes fondos, equipo y programas de computadora y ayudarlas con el mantenimiento de los sistemas de computadoras de las universidades; ofrecer formación en sitio a los miembros de la facultad, incluidos los que no tienen experiencia previa en seguridad de la información, y dotar becas para estudiantes que deseen trabajar en este sector.

El NCISSE insta al gobierno a elaborar y compartir cursos en seguridad de la información y propiciar el establecimiento de centros universitarios de protección de la infraestructura según el modelo de los centros de materiales

patrocinados por la National Science Foundation y los centros de transportes patrocinados por el Departamento del Transporte.

Los miembros del Coloquio piden a los profesionales de la información de todo el país que mejoren las redes que conectan entre sí al personal docente, patrocinen más conferencias sobre seguridad de la información, abran más espacios en la Web, y publiquen más revistas sobre protección de las redes de información de Estados Unidos. También subrayan la necesidad de establecer un sistema oficial de reconocimiento de programas educativos sobresalientes en seguridad de la información.

En cuanto a las instituciones de educación superior, el NCISSE las exhorta a aumentar los programas que se concentran en los componentes de seguridad de la información y a incluir cursos sobre este tema en los programas de estudio básicos de todos los estudiantes de colegios universitarios.

De especial importancia es la inclusión de programas de estudio que abordan las cuestiones éticas y culturales planteadas por los sistemas modernos de información, en particular cómo se mantienen los valores tradicionales en la era de la información moderna y cómo puede ser necesario cambiarlos.

Dado que muchos de los valores éticos y culturales se adquieren en una etapa temprana de la vida, se insta a las instituciones de enseñanza superior a elaborar programas de estudios de seguridad de la información para estudiantes de enseñanza secundaria, en colaboración con los responsables de ese ciclo de estudios.

En reconocimiento de que la educación superior es por sí misma una profesión dirigida por normas, se insta a las instituciones docentes a solicitar orientación a las entidades de acreditación en cuanto al lugar apropiado que debe ocupar la seguridad de la información en sus programas de estudio.

Por último, debido al interés por la educación continua en una sociedad tecnológica en rápido proceso de evolución, se insta a las instituciones

de enseñanza superior a ofrecer programas de educación continua para profesionales de la seguridad de la información que ya trabajan en el sector.

El Coloquio recomienda que los educadores de seguridad de la información elaboren e intercambien ejercicios prácticos de laboratorio sobre la materia, diseñen juegos de computadora que expresen valores apropiados para una fuerza laboral responsable y con conocimientos de informática, establezcan un lugar para compartir material de instrucción y escriban más libros de texto, sobre todo referentes a cuestiones prácticas.

El programa de acción del NCISSE también pide a los especialistas en educación jurídica que ayuden a los abogados de Estados Unidos a comprender la seguridad de la información

Métodos basados en la Internet

La urgente necesidad que existe en el país de profesionales de seguridad de la información es característica del mundo tecnológico moderno. Como resultado de la rápida evolución de la tecnología, los profesionales deben comprometerse a seguir aprendiendo a lo largo de toda su vida para poder renovar y ampliar constantemente sus conocimientos. Todos los profesionales tienen que estar preparados para dar nuevo rumbo a sus carreras y adquirir nuevos conocimientos, ya que los cambios tecnológicos imponen nuevas necesidades de fuerza laboral.

La necesidad de profesionales de la información ha aumentado vertiginosamente en los últimos años. En consecuencia, se ha producido un correspondiente aumento de la demanda de oportunidades educativas para formar nuevos profesionales y orientar a los actuales en una nueva dirección. No obstante, no es razonable esperar que esos profesionales que buscan educación continua interrumpan su carrera y su vida familiar para cursar estudios en una universidad tradicional. Esta circunstancia, la necesidad de disponer de programas de educación continua para profesionales que no pueden interrumpir su carrera o su vida familiar, es lo que ha provocado el enorme interés que existe actualmente en la educación a través de la Internet. La Universidad James Madison ha

respondido a esta necesidad y a la tecnología de la Internet con un programa profesional a nivel graduado de seguridad de la información.

El programa de estudios se ofrece a través de la Internet mediante contratos con organizaciones que pueden garantizar la integridad de los procedimientos de examen a que se someten sus empleados.

El programa está estructurado en 13 cursos de siete semanas cada uno y tiene una duración de algo más de dos años. Un grupo de estudiantes, lo que se conoce como una cohorte, empieza el programa, sigue, uno tras otro, los 13 cursos, y llega al final.

Este programa de la Internet combina el estudio independiente con la instrucción dirigida y la colaboración en grupo, coordinada por una dependencia central encargada de prestar una serie de servicios. Los profesores y la tecnología constituyen un sistema que mantiene altas normas académicas al mismo tiempo que es flexible y tiene en cuenta las necesidades de los participantes. Grupos de debate examinan, discuten y evalúan por medios electrónicos conceptos de seguridad de la información. Cada curso consiste en una serie de lecturas y solución de problemas.

Se puede llegar a las presentaciones del curso desde cualquier computadora conectada a la Internet en cualquier parte del mundo y en cualquier momento. Los proyectos presentados en cada clase ofrecen orientación práctica sobre conceptos y materiales de estudio.

El programa de seguridad de la información de la Universidad James Madison

Los participantes que completan los programas de seguridad de la información de la Universidad James Madison reciben una licenciatura en ciencias de la informática, especializada en seguridad de la información. El programa se basa en una norma respaldada por la Agencia Nacional de Seguridad y está diseñado para impartir los conocimientos y las aptitudes necesarios para comprender las relaciones mutuas entre seguridad de la información y tecnología de la información y relacionar los componentes técnico y humano de la seguridad

de la información y la tecnología de la información.

Los cursos giran en torno a la administración, gestión, evaluación y puesta en práctica de la tecnología de la informática, con un acento especial en la seguridad de la información. Los programas de gestión de la seguridad de la información incluyen el mantenimiento y la protección del secreto, la integridad, disponibilidad, autenticidad y utilidad de la información dentro de límites aceptables de riesgo.

Los miembros del programa trabajan en equipos

— Desarrollan las aptitudes y los conocimientos necesarios para comprender las relaciones entre la seguridad de la información y el adelanto de las tecnologías de los sistemas de información necesarios para llevar a la práctica programas de detección y prevención del delito;

— Adquieren un elevado grado de competencia en aspectos técnicos, normativos, de supervisión y otros afines, de la seguridad de la información y la tecnología de la informática con respecto a la evaluación de vulnerabilidades, amenazas y riesgos;

— Adquieren perspectivas que necesitan los analistas, gestores, administradores y profesionales de la seguridad de la información en la planificación, evaluación y puesta en práctica de técnicas y programas de seguridad de la información;

— Vinculan los componentes técnico y humano de la seguridad de la información y la tecnología de la informática en la protección de los sistemas de información;

— Adquieren competencias básicas en diseño de bases de datos y sistemas de información, sistemas y redes de operación, y elaboración de programas de computadoras destinados a mejorar la capacidad de investigación y prevención del delito.

El programa comienza con un segmento preparatorio para quienes necesitan perfeccionar sus conocimientos en materia de computadoras antes de comenzar con el curso básico de informática. A esta fase le siguen tres cursos de informática que tratan de gestión de bancos de datos, sistemas y redes de operación y elaboración de programas de computadora. Sobre esta sólida base se presenta, en el tercer período, la seguridad de la información, conceptos de sistemas de información fiables y técnicas seguras de almacenamiento y transmisión de información, en particular mediante criptografía. El cuarto segmento se dedica a administración y cuestiones afines en relación con la seguridad de la información, incluido el análisis de riesgo y vulnerabilidad, instrumentos y procedimientos de auditoría de los sistemas de información y cuestiones jurídicas, éticas y normativas. Un ejercicio final integra todo el programa en un proyecto en el que se ponen a prueba las aptitudes de los participantes en el análisis de la seguridad de un sistema de información.

El Programa de Estudios de Seguridad de la Información de la Universidad James Madison

El Programa de Estudios de Seguridad de la Información de la Universidad James Madison incluye los siguientes cursos, organizados en segmentos:

1. Segmento de informática básica

Sistemas y redes de operación — Conceptos y principios de sistemas de operación de múltiples usuarios. Memoria, unidad central de proceso, dispositivo de asignación de entrada/salida, planificación y seguridad. Jerarquías de memorias, evaluación de resultados, modelos analíticos, simulación, programación simultánea y procesadores en paralelo.

Sistemas de gestión de bancos de datos — Tipos de métodos de almacenamiento y acceso físicos; modelos de datos, álgebra y cálculo por relaciones y lenguajes de definición y de consulta; dependencias, descomposición y normalización; diseño de bancos de datos; recuperación, coherencia y simultaneidad; bancos de datos distribuidos. Ejemplos de bancos de datos comerciales.

Elaboración de programas de computadora — El ciclo de vida de la elaboración de programas de computadora, administración de proyectos de programas de computadora, instrumentos y procedimientos de elaboración, garantía de calidad de los programas de computadora, paradigmas del lenguajes de programación y su uso en la elaboración de programas de computadora.

2. Segmento técnico de la seguridad de la información

Introducción a la seguridad de la información — Panorama general de las amenazas a la seguridad de los sistemas de información, responsabilidades, instrumentos básicos de la seguridad de la información así como para la capacitación y la insistencia necesarias en las organizaciones para alcanzar y mantener un nivel aceptable de seguridad.

Sistemas fiables — Definición de "sistema fiable" y consideraciones de diseño, evaluación, certificación y acreditación de sistemas fiables, incluidas las consideraciones de componentes físicos y programas de computadora tales como controles de elaboración, convalidación/verificación, distribución asegurada y otras cuestiones de garantía. Administración de configuración, aplicación, y administración de sistemas fiables. La importancia de entender la psicología y el modus vivendi exitoso del atacante, a fin de para generar y mantener una defensa eficaz.

Criptografía — En este curso se dan al estudiante los conocimientos y la capacidad de aplicar importantes protocolos de criptografía. En él se tratan cuestiones tales como diseño y análisis de sistemas de protección de comunicaciones o resistencia al análisis criptográfico.

3. Segmento de administración de la seguridad de la información

Análisis del riesgo y la vulnerabilidad de los sistemas de información — Se identifican y estudian las vulnerabilidades y los riesgos intrínsecos al funcionamiento y la administración de los sistemas de información.

Controles de auditoría de la seguridad de la información — Los estudiantes elaboran planes y llevan a cabo una auditoría de seguridad de la información, que incluye un estudio a fondo de la seguridad física. Elaboran y aplican normas para vigilar las actividades normales de un sistema de información.

Políticas, procedimientos, cuestiones jurídicas y éticas — Elaboración, evaluación y aplicación de normas y procedimientos administrativos de seguridad en un sistema UNIX en un entorno seguro. Preparación de una Guía administrativa de seguridad o un anexo a dicho documento.

4. Ejercicio final de seguridad de la información

Un ejercicio final integra todo el programa en un proyecto que pone a prueba la capacidad de los participantes de analizar la seguridad de un sistema de información, estudiar y analizar la eficacia de opciones existentes para mejorar la seguridad, examinar el contexto jurídico y ético más amplio de estas opciones y seleccionar y proponer un procedimiento de aplicación de una de ellas.

Clases preparatorias — Los estudiantes que no están preparados para comenzar a trabajar con el material básico pueden matricularse en una serie de tres clases preparatorias consecutivas: Principios fundamentales acelerados de la programación de computadoras, Principios fundamentales avanzados de la programación de computadoras y principios fundamentales acelerados de sistemas computarizados.

LOS SECTORES PRIVADOS Y PUBLICOS SE BENEFICIAN AL COMPARTIR SU EXPERIENCIA EN ASUNTOS DE SEGURIDAD

Entrevista con Howard Schmidt, director de Seguridad Informática de Microsoft Corporation

(Las agencias gubernamentales y muchas compañías privadas tienen ahora la capacidad “de entrar en contacto y sostenerse entre sí” en el caso de amenazas a su información o a otros sistemas esenciales, afirma Howard Schmidt, director de Seguridad Informática de Microsoft Corporation. Menciona también la extensa cooperación que existe entre las compañías para abordar cuestiones de ataques informáticos.

“Cuando se trata de asuntos de seguridad, son muy pocas las cosas que tienen que ver con la competencia”, dice Schmidt. “Colaboramos igualmente con nuestros competidores y asociados para ayudar en los adelantos regulares, de modo que todos tengamos éxito en desarrollar y mantener la seguridad”. Entrevistó a Schmidt la directora Dian McDonald).

PREGUNTA: ¿Cómo estima usted la vulnerabilidad de las infraestructuras norteamericanas esenciales en caso de un ataque cibernético? ¿Cuán preparado está Estados Unidos para resistir tales ataques?

SCHMIDT: Mi estimación es compatible con la de la Comisión Presidencial sobre Protección de Infraestructuras Esenciales: tenemos trabajo para hacer. Estas eran cuestiones que, al establecerse esta comisión, no figuraban realmente en primer plano. En cuanto a nuestra capacidad de resistir esos ataques, creo que la Comisión Presidencial sobre Protección de Infraestructuras Esenciales ha hecho mucho para que los sectores privados y públicos, colectivamente, puedan resistir estos tipos de ataques y, básicamente, puedan responder bien a ellos.

P: ¿Ha trabajado usted con la comisión?

SCHMIDT: Sí, hemos trabajado con la comisión. Ellos estuvieron aquí (en Redmond, estado de Washington) para un par de reuniones. Y yo estuve en Washington D.C. para un par de reuniones. De hecho, estamos organizando una reunión bastante grande de gente del gobierno y del sector privado, con el fin de que se llegue a

un acuerdo sobre las maneras de crear una infraestructura mejor.

P: ¿Qué cambios de organización ha hecho su compañía por causa de las nuevas amenazas a la tecnología?

SCHMIDT: Permítame plantear esta pregunta de otra manera, porque nosotros no lo consideramos una amenaza a la tecnología. Nosotros, como quien dice, lo vemos como la utilización de una tecnología que le da a alguien la oportunidad de hacer algo en contra de un público más amplio. Básicamente, consideramos que se trata de las mismas amenazas de siempre, pero que se está utilizando la tecnología nueva.

En respuesta a eso, hace un año hemos creado un programa del que estamos muy orgullosos: el MIAP, o Programa Microsoft de Seguridad Informática, que nos da la capacidad de unir internamente muchos de los intereses que se relacionan con proteger nuestra información o aseguran que nuestra información sea válida. Tenemos ahora bajo una organización “general” varios programas y funciones, que incluyen nuestro plan de recuperación en caso de desastre, nuestra retención de datos y nuestro sistema de clasificación, nuestra estrategia de

respaldo, el mismo grupo para la seguridad informática, el grupo para la seguridad física tal como se relaciona con la seguridad informática, así como el grupo para la seguridad del producto, puesto que Microsoft es un productor de programas de computación.

Conforme a esta estructura tenemos un intercambio de información y una utilización combinada de todas las especialidades, no solamente para asegurar nuestra información y nuestros sistemas, sino para cerciorarnos de que los productos que desarrollamos se benefician de la experiencia de aquellos en el terreno de la seguridad informática, para ayudarles a hacer que los productos sean mejores.

P: En términos de estrategias para abordar los ataques informáticos, ¿en qué medida trabaja usted en concierto con otras compañías?

SCHMIDT: Mucho. De hecho, tenemos un número de grupos diferentes: como la Asociación de Seguridad de Sistemas Informáticos, una organización sin fines de lucro cuyos miembros están involucrados en el terreno de la seguridad — por ejemplo, representantes de Charles Schwab Company; U.S. Space Alliance; Air Touch Cellular, y varias agencias gubernamentales. Participamos en conferencias y colaboramos con el Grupo Gartner, una gran firma consultora en materia de computación. Participamos en la iniciativa del ex senador Sam Nunn, quien ha sido coadyutorio en el terreno de la protección infraestructural. El coordina un foro sobre seguridad que se celebra periódicamente en el Instituto de Tecnología de Georgia, en Atlanta, y también hemos participado en ese foro.

Por lo tanto, existe mucho intercambio de información, la mejor práctica entre nosotros en el terreno de la seguridad, en el sector privado. Y hay otros grupos, como el Federal Computer Investigations Committee y la High Tech Crimes Investigator's Association, integrados por representantes tanto del sector público como privado que colaboran en este terreno. Por lo tanto, tenemos algunas relaciones realmente buenas, y colaboramos muy estrechamente.

Tratándose de cuestiones de seguridad, son muy pocas las cosas que se relacionan con la competencia. Colaboramos igualmente con

nuestros competidores y asociados para ayudar en los adelantos regulares, de modo que todos tengamos éxito en desarrollar y mantener la seguridad.

P: ¿Puede usted explayarse sobre cómo su organización colabora con el sector gubernamental en hacer frente a nuevos retos a los sistemas informáticos?

SCHMIDT: Tenemos un par de medios nuevos. Naturalmente, aquellos que crean los productos que todos utilizamos, mantienen vínculos muy, muy estrechos con los funcionarios en todas las agencias gubernamentales, para asegurar que los productos sean fabricados de modo que satisfagan las necesidades del gobierno en lo que se refiere a asegurar la infraestructura esencial.

Del otro lado de esto, como proveedores de servicios en línea, nosotros mismos también formamos parte de la infraestructura y colaboramos muy estrechamente, por ejemplo, en proveer experiencia técnica para ayudar a aquellas personas que llevan a cabo investigaciones en línea. Tenemos ahora un número de teléfono para casos de emergencia, las 24 horas del día, los siete días de la semana, para uso de las autoridades de ejecución de la ley, en lo que se relaciona con investigaciones de personas que cometen actos ilegales en la Internet.

También sostenemos reuniones periódicas sobre prácticas óptimas. Hacemos muchas presentaciones en reuniones del gobierno. Por ejemplo, hace algunos meses pronuncié un discurso de apertura en la Universidad de Defensa Nacional, en la ciudad de Washington. Asistí a la Conferencia "Defending Cyberspace '98" (Conferencia 1998 para la Defensa del Espacio Cibernético), que tuvo lugar en Washington en septiembre pasado. Nosotros participamos en estos tipos de foros, y compartimos nuestras experiencias mutuas para el mejoramiento de todos los que estamos en este terreno.

P: ¿Cree usted que el gobierno debería desempeñar un papel más prominente en proteger las infraestructuras esenciales y, de ser así, en su opinión, cuál podría ser este papel?

SCHMIDT: Básicamente, creo que el gobierno debería seguir trabajando en colaboración con el sector privado. Creo que la Directiva de Decisión Presidencial 63 (PDD 63), con la que se creó la Oficina para Seguridad de Información Esencial, provee la estructura apropiada para colocar al gobierno en una buena posición para trabajar con el sector privado. Y creo que con este papel gubernamental — sin legislación nueva o reglamentos nuevos — podremos ir más lejos al trabajar con el gobierno, a fin de asegurar que las infraestructuras esenciales sigan siendo en efecto un recurso protegido.

P: ¿Ve usted en Estados Unidos conflictos filosóficos entre las necesidades informáticas de las compañías y los intereses gubernamentales en lo que se refiere a la seguridad?

SCHMIDT: Básicamente no veo que haya un conflicto. Creo que lo que vemos en ese sentido es que todos queremos asegurarnos de que exista la máxima seguridad y que al mismo tiempo se proteja la confidencialidad de nuestra información corporativa, la información gubernamental, la información personal y cosas de esa naturaleza. Si bien puede haber algunas diferencias en lo que se refiere a cómo abordamos los problemas, creo que el punto crítico es el hecho de que todos estamos de acuerdo con que debemos trabajar en colaboración para asegurar que la infraestructura esté protegida.

P: ¿Cómo pueden colaborar mejor los sectores públicos y privados para desarrollar capacidades efectivas de defensa contra ataques terroristas u otros actos hostiles?

SCHMIDT: Creo que ya me he referido a eso, pero lo principal es que ahora tenemos, con varias agencias del gobierno y muchas compañías diferentes, la capacidad de entrar en contacto y sostenernos los unos a los otros en el caso de que ocurriera algo como esto. Y creo que estamos bien preparados para proveer experiencia técnica a las organizaciones de sostén de las autoridades de ejecución de la ley. Obviamente, seguimos trabajando para encontrar las maneras de institucionalizar y formalizar más estos procedimientos, pero nos veo haciendo

esto ahora y que continuaremos haciéndolo y que lo haremos mejor.

P: ¿En qué forma integra Microsoft en sus productos el elemento de seguridad para ayudar a que sus clientes se protejan a sí mismos?

SCHMIDT: Esto es algo que está más allá de mi área de responsabilidad, pero puedo decirle que representantes de Microsoft se reúnen regularmente con sus clientes. A todos nos preocupa la seguridad. Los empleados de Microsoft encargados del desarrollo de productos trabajan constantemente para cerciorarse de que todos sus productos ofrezcan una mayor seguridad, y trabajan con nosotros y con los expertos en seguridad informática, puesto que nosotros utilizamos aquí nuestros propios productos. Por lo tanto, existe un constante intercambio informativo, lo que asegura que los productos sean todo lo seguros que puedan serlo ahora — y en el futuro, a medida que se descubran nuevas vulnerabilidades.

P: ¿Cree usted que con los controles tecnológicos actuales, es posible protegerse ahora de los virus de computadoras y de los terroristas cibernéticos?

SCHMIDT: Recientemente ha habido mucha publicidad acerca de los diferentes virus y de otras cosas. Obviamente, ocurre lo mismo que con cualquier otro tipo de actividad ilícita, al descubrirse estas cosas. Nosotros en el sector privado y el gobierno trabajamos conjuntamente para contrarrestarlos y para asegurarnos de que estemos prevenidos contra estas amenazas, y miramos hacia el futuro para tratar de predecir lo que alguien pudiera querer hacer. Mientras sigamos compartiendo la información y tengamos los grandes sistemas informáticos de los que todos dependemos, habrá quienes tratarán de hacer algo contra esos sistemas. Pero lo principal es que con la tecnología, la educación humana y el conocimiento de los riesgos, creo que podremos manejar bien cualesquiera de los aspectos protectores que están relacionados con ellos.

P: ¿Desarrollaron ustedes alguna tecnología que pueda proteger a una compañía de un diluvio inexorable de mensajes electrónicos enviados por algún terrorista cibernético?

SCHMIDT: Sí. Existe un número de recursos y perfeccionamientos que hemos integrado en nuestros productos, y que otras compañías han puesto en sus productos, para aliviar este tipo de problema. También, algunas compañías con las que trabajamos conforme a nuestro Programa de Asociados en Cuestiones de Seguridad, han

desarrollado algunas herramientas muy, muy buenas — cuando digo herramientas me refiero a programas de computadora — que realmente ayudarán a protegerse contra ataques de denegación de servicio y bombas de correo electrónico y cosas por el estilo. Hemos progresado mucho en arreglar este problema.

ESTRATEGIAS PARA CONTRARRESTAR LAS AMENAZAS A LOS RECURSOS DE TECNOLOGIA DE INFORMACION

Por James A. Lingerfelt
Consultor principal, IBM, Seguridad Pública y Justicia

(La amenaza primordial a los sistemas de información no es el maligno “intruso cibernético” dotado de capacidades formidables, dice Lingerfelt, experto en tecnología y planeación estratégica para la ejecución de la ley. “Más bien, los mayores peligros a los sistemas de computadoras y bancos de datos son las fuentes `confiables”. El autor hace hincapié en que “una evaluación realista de las necesidades y amenazas en materia de seguridad, seguida de una formulación y aplicación significativas de un plan de seguridad, puede brindar protección efectiva contra la gran mayoría de las amenazas, y a un costo razonable”. Lingerfelt identifica las áreas que son fuentes más frecuentes de amenazas reales y presenta siete estrategias básicas para la planeación de la seguridad de la tecnología de información).

Las agencias de ejecución de la ley y justicia penal tienen una oportunidad sin precedentes de usar tecnología de información (TI) para transformar sus operaciones y proveer un servicio mejor y más efectivo. Sin embargo, muchas agencias se muestran reacias a aprovechar la oportunidad porque temen que al reemplazar o complementar sus sistemas de estructura central cerrada con computadores personales vinculados en una red, y poner en práctica informes automatizados y redes de computadoras, se expondrían a sí mismos a los ataques de los intrusos cibernéticos. Los costos estimados elevados de proteger todos los sistemas de TI de la penetración de los intrusos cibernéticos, combinado con el daño que podría resultar de la pérdida de información extremadamente confidencial, hacen que parezca razonable evitar lo que se percibe como un riesgo, a pesar de las ganancias a obtener mediante el uso de la TI.

Es un hecho que, debido a los aumentos exponenciales del uso de la TI, hay una exposición creciente a los ataques a los sistemas y activos informáticos y bancos de datos. Sin embargo, el temido y bien informado intruso cibernético es raramente la amenaza mayor. Más bien, los mayores peligros que amenazan a los sistemas de computadoras y bancos de datos son las fuentes ‘confiables’ Una evaluación realista de las necesidades y

amenazas en materia de seguridad, seguida de una formulación y aplicación significativas de un plan de seguridad, puede brindar protección efectiva contra la gran mayoría de las amenazas, y a un costo razonable.

PERCEPCION VS. HECHOS

Muchos departamentos han comprometido a la TI recursos financieros sustanciales. Esto ha ido acompañado de un aumento en el número de informes sobre ataques de los intrusos cibernéticos a los sistemas de información policial.

Aumentan también los informes sobre uso ilegal de información procedente de bancos de datos policiales, robos de información policial y robos de recursos de TI pertenecientes a agencias policiales. La frecuencia de estos informes ha desalentado a muchas agencias policiales de aventurarse más allá de sus sistemas cerrados ya existentes. Sin embargo, los nuevos requisitos empresariales impuestos a las agencias de justicia penal exigen que cambien los métodos mediante los cuales obtienen, comparten y diseminan información.

Se han iniciado cambios operativos como resultado de la necesidad de distribuir en el terreno los sistemas de información, modernizar

los procesos de trabajo, distribuir información más allá de los límites de la organización o intercambiar información con agencias e individuos fuera de tales límites.

Algunas agencias han respondido usando personal que se ocupa de las nuevas tareas, con lo cual se sustrae personal de la fuerza disponible. Otros han puesto en práctica nuevos sistemas "separados" que proveen solamente los nuevos servicios, pero no están integrados con los que ya posee la agencia ni son complementarios de éstos. Esto sólo consigue aumentar la complejidad y costo — en personal, tiempo y dinero — del apoyo a la TI.

Como ya se observó, las amenazas internas provenientes de fuentes dentro del dominio confiable causan más daño que los intrusos. Han sido documentados varios incidentes causados por fuentes internas:

— La red de todo un departamento colapsó por causa de un virus contenido en diskettes que la división de planeación del departamento distribuyó para recoger información de encuestas.

— El jefe de inteligencia que supervisaba un sistema de inteligencia jerárquico dejó escritos en su pantalla su identificación de usuario y su contraseña, con instrucciones detalladas para entrar en la red.

— Un alto funcionario de un departamento de policía vendió a representantes del crimen organizado un documento que contenía la descripción y las placas de todos los automóviles no identificados que utilizaban los agentes de policía.

— Un administrador de red novato que instalaba una red en un departamento de policía les dio a todos los usuarios privilegios de administrador.

— A los programadores de aplicación en un importante departamento de policía se les permitió colocar directamente en uso un nuevo código de programa directamente, sin probarlo ni examinarlo, y todo el sistema colapsó durante 24 horas como resultado del código incorrecto.

— Un gobierno estatal abrió un sitio en la Web que carecía de cortafuegos. En 24 horas,

el documento que contenía la identificación y la contraseña de usuario estaban a disposición de los intrusos cibernéticos. El estado, hay que reconocerlo, compartió la experiencia con otros estados y, en consecuencia, los ayudó a evitar cometer el mismo error.

Ninguno de estos casos involucra a un intruso cibernético dotado de capacidades extraordinarias que ataca con éxito los sistemas de información de una agencia. El último ejemplo es una penetración posibilitada por la peor de todas las aberturas posibles. Todos estos incidentes podrían haberse prevenido mediante un poco de planeación, entrenamiento y supervisión básicos.

En suma, hay, como resultado del uso cada vez mayor de la tecnología de la información, una amenaza creciente de ataques provenientes del exterior, pero la proporción de la amenaza en relación con el todo no ha cambiado — sólo el todo es más grande. ¿Es mayor la amenaza? Sí. ¿Es diferente? No.

El aumento de exposición a las amenazas a la seguridad de las computadoras se debe a varias causas:

— Nuevos modelos de empresa: el sector público imita al sector privado, con un retraso de alrededor de cinco años.

— Crecimiento exponencial del uso de la TI: las computadoras y las redes se han infiltrado en casi todos los aspectos de nuestra vida.

— Costos reducidos: Hoy, la tecnología es barata. No importa la medida que se utilice, los costos de la TI básica son más bajos que nunca, y el costo de la nueva tecnología disminuye más rápidamente que hace apenas unos pocos años debido a los rápidos adelantos y el aumento de la competencia.

NUEVOS MODELOS DE EMPRESA

En la transición de las operaciones centralizadas a las operaciones descentralizadas, las sedes centrales de la toma de decisiones y el universo de la información han sido reemplazadas por unidades empresariales independientes y a distancia, apoyadas por una distribución de TI.

Para la TI este cambio ha significado una transición de las arquitecturas cerradas a las redes — redes internas y externas. La distribución de la información significa más dificultades para proteger sistemas, vigilar operaciones y responder a problemas. Hay más puntos expuestos. Lo bueno es que la distribución de TI hace posible enormes ganancias en productividad — y el rendimiento de la inversión ocurre a menudo menos de un año después de hacerla.

Las organizaciones del sector privado han comenzado a concentrarse en la competencia especializada en lugar de proveer de todo a todo el mundo. Las empresas mantienen un personal mucho más pequeño. Esto les permite evitar problemas laborales y logísticos vinculados con los cambios. Sólo se cubren los puestos que contribuyen directamente a alcanzar las metas empresariales. Las fusiones y adquisiciones reclaman frecuentemente que se recurra a fuentes exteriores para ocuparse de las funciones de apoyo y administrativas, en particular la TI. Las agencias de justicia penal (y todo el gobierno) han comenzado a avanzar en la misma dirección para modernizar operaciones, reducir costos y mejorar servicios.

Además, retener el personal capacitado en TI se ha vuelto muy difícil. Los gobiernos no han podido competir con los salarios del sector privado para reemplazar el personal que pierden. Esto también ha aumentado el uso de fuentes exteriores por parte del gobierno.

La creciente rotación de ejecutivos y gerentes es otra realidad en las organizaciones de hoy. A medida que las compañías se reducen en tamaño, o incursionan unas en otras en busca de expertos, se plantea la amenaza de que los ejecutivos o los gerentes de nivel intermedio se lleven consigo propiedad intelectual importante. Un caso semejante se llevó con éxito ante la justicia cuando se demostró que la estructura de directorio incluida en los documentos de computadora de un gerente era idéntica a la que había en la unidad empresarial a la que el gerente había pertenecido anteriormente. El hecho de que las compañías que reducen su tamaño a menudo pierden millones de dólares en equipos

de computadora, programas de computadora, existencias y muebles robados, si a los empleados se les avisa anticipadamente de la reducción, raramente se reconoce o se da a conocer.

A pesar de los beneficios que representa, utilizar recursos exteriores de TI puede resultar en riesgos de seguridad. Es especialmente importante contar con un plan de seguridad cuando las responsabilidades de TI que son esenciales para la misión de la empresa han de transferirse a empleados por contrato o personas fuera de la agencia. La agencia puede exigir que todos los empleados por contrato cumplan con ciertos requisitos de investigación de antecedentes.

CRECIMIENTO EXPONENCIAL DEL USO DE LA TECNOLOGIA DE LA INFORMACION

Las computadoras y las redes computarizadas se han infiltrado en casi todos los aspectos de nuestras vidas. El fraude, el robo y la diseminación ilegal de información y materiales son posibles gracias a las computadoras, las redes computarizadas y la Internet que todos usamos. Se conciben nuevos crímenes y se insufla nueva vida a los viejos esquemas.

Afortunadamente, este aumento del uso de las computadoras ha generado adelantos en tecnología, estándares e identificación de las prácticas óptimas. A medida que las lecciones aprendidas de los errores han mejorado la tecnología, todos nos hemos beneficiado. Las prácticas de seguridad también han mejorado en reacción directa a las lecciones aprendidas, y ha surgido un conjunto sólido de prácticas óptimas. El sector privado ha allanado el camino. La mayoría de los productos nuevos (tanto de equipos como de programas de computadora) incluyen dispositivos de seguridad funcionales. Que las funciones se usen o no, es otra cuestión.

COSTOS REDUCIDOS

No importa la medida que se use, los costos de la TI básica son más bajos que nunca. Casi todo el mundo puede comprar una computadora.

No sólo la TI cuesta menos, en el sector público hay más dinero disponible para invertir en TI que en cualquier momento desde fines de la década de los 60 y principios de la de los 70. Por ejemplo, las iniciativas relacionadas con el problema de computadoras del año 2000 y el crimen computarizado proveen miles de millones de dólares con el propósito expreso de mejorar o reemplazar los sistemas de información del sector público. Esto crea una oportunidad perfecta para que las agencias de justicia penal incluyan la seguridad en el desarrollo y puesta en práctica de procesos empresariales y sistemas de TI nuevos. Tratar de introducir mecanismos de seguridad en sistemas existentes es demasiado caro y, por lo general, no da resultado.

PLANEACION DE LA TECNOLOGIA DE INFORMACION

El libro de ciencia ficción “Guía para los que Quieren Hacer Auto Stop hasta la Galaxia”, presenta como su primera regla:

NO SE DEJE LLEVAR POR EL PANICO. Este es también un buen consejo para la planeación de seguridad de la TI. Muchas organizaciones se han resistido a invertir en TI debido a la creencia, persistente y exagerada, de que de inmediato las asediarán los intrusos cibernéticos y los entrometidos.

A pesar de la creciente exposición y el creciente número de intrusos potenciales, hay disponibles experiencia y herramientas para construir defensas efectivas y mejorarlas continuamente. Con una planificación anticipada efectiva, es posible responder rápida y apropiadamente a cualquier ataque, prevenir la mayoría de ellos y minimizar el efecto de los demás.

La planeación general debe hacerse teniendo presente el cuadro amplio: el plan de TI debe fluir directamente de los planes operativos de la organización. El plan debe describir los requisitos empresariales que satisfarán las metas operativas: no es una lista de deseos computarizada. Hay que concentrarse en lo que se necesita hacer, no en cómo se lo hará. Por lo común hay muchas maneras de satisfacer un requisito, y entre ellas hay grandes diferencias en costo. Debe haber una justificación clara para cada dólar que se gaste. Y, desde el comienzo, hay que incluir la seguridad en el plan de TI.

Las arquitecturas deben mantenerse simples. Esto ofrece una ventaja importante en materia de seguridad. Los sistemas múltiples, no importa cuán estrechamente estén integrados, ofrecen puntos de acceso múltiples y requieren administración de seguridad y sistemas de apoyo múltiples que se traducen en costos incrementados.

SIETE ESTRATEGIAS PARA GARANTIZAR LA SEGURIDAD EN LA TECNOLOGIA DE LA INFORMACION

1. POR ENCIMA DE TODO — MANTENERLO SIMPLE. Si el sistema es muy complicado, los usuarios lo evitarán o tratarán de darle un rodeo, con lo que se anularán las medidas de seguridad y se reducirá su utilidad. Las medidas de seguridad modernas pueden ser efectivas sin interferir.

2. DESARROLLAR POR ADELANTADO POLITICAS, PROCEDIMIENTOS Y SANCIONES(P3). Diseñar un sistema de seguridad P3 que se base en las necesidades del usuario, la naturaleza de las aplicaciones y la información que se asegura. APLICARLAS constantemente. Tener unas P3 que no se aplican es peor que no tener ninguna.

3. OFRECER ENTRENAMIENTO EN EL USO DEL SISTEMA Y HACER HINCAPIE EN LAS P3. Reforzar el adiestramiento mediante el examen y distribución de material noticioso relevante — por ejemplo, relatos relacionados con ataques cibernéticos o abusos de sistemas.

4. TANTO COMO SEA POSIBLE, USAR PRODUCTOS DE SEGURIDAD DISPONIBLES EN EL COMERCIO, MAS BIEN QUE DESARROLLAR INTERNAMENTE APLICACIONES DE SEGURIDAD. Esto es aconsejable por varias razones, porque las necesidades empresariales son relativamente simples. Las agencias de justicia penal asocian personas entre sí y personas con acontecimientos, recopilando y compartiendo información. Los productos estandarizados basados en estándares abiertos han sido probados y aprobados, y se puede entrevistar a sus clientes y aprender de ellos. Incluso si los productos son nuevos, las metodologías usadas para probarlos pueden evaluarse y examinarse los resultados. Lo más importante de todo es

que los productos estandarizados de la industria están, de modo típico, bien documentados para que los empleen los usuarios y el personal técnico de TI. La documentación y el ensayo de seguridad se descuidan frecuentemente cuando las aplicaciones se desarrollan internamente.

5. DIVIDIR EN COMPARTIMIENTOS LA INFORMACION, LOS SISTEMAS Y LOS USUARIOS. PROTEGER APROPIADAMENTE LA INFORMACION Y LOS SISTEMAS DE ACUERDO CON SU VALOR. Los informes de inteligencia confidenciales deben estar protegidos mediante una seguridad elevada. La información que es pública y/o puede ser reemplazada fácilmente no requiere, sin embargo, una seguridad refinada. Una evaluación objetiva de los sistemas de información mostrará que una cantidad mucho mayor de ellos son públicos en lugar de confidenciales.

De modo similar, los elementos de TI (computadoras personales, servidores, tarjetas de red, cables, etc.) y los suministros (programas de computadora, diskettes, etc.) deben inventariarse y asegurarse apropiadamente. Frecuentemente, las agencias reciben grandes cantidades de equipo físico y programas de computadora (computadoras personales, monitores, tarjetas de acceso a la red, bocas de conexión en paneles de control, dispositivos que conectan dos redes de área local, etc.) sin anotar esos artículos en un banco de datos de control de activos, y sin verificarlos cuidadosamente para garantizar que son lo que se pidió y que los artículos están configurados correctamente y funcionan apropiadamente. Cuando se pierden los artículos o no funcionan apropiadamente, no hay constancias para demostrar la pérdida o que el sistema no funciona como se requiere. La administración de inventario es un primer paso. El segundo es el control de configuración.

En el momento en que se la recibe, debe establecerse la configuración cada pieza de equipo físico y cada programa de computadora debe quedar apropiadamente registrado. El inventario contendrá, entonces, una descripción detallada de cada uno de los componentes del sistema, tanto equipo físico como programas de computadora, y de dónde están ubicados (hasta llegar al número de la oficina y escritorio). Esta información es de valor inapreciable para la protección de los activos informáticos, la

identificación del robo o la manipulación y la realización de investigaciones efectivas cuando se descubren problemas. Hay disponibles programas de computadora que verifican la configuración e informan automáticamente acerca de problemas a los administradores de seguridad. Estos programas mantienen también un registro de cambios o de mantenimiento del sistema. Según se van haciendo reparaciones, se introducen mejoras en los sistemas o se les presta mantenimiento, es importante que se deje constancia de tales actividades. Finalmente, las cerraduras y tornillos especializados para cerrar las estaciones de trabajo pueden reducir el robo o la manipulación. La política de la agencia debería requerir que se informe de todos los problemas que parezcan sospechosos para proceder a investigarlos.

La división en compartimientos de los suministros y activos cibernéticos significa que hay que tratarlos apropiadamente, según su costo o la importancia que tengan para la misión de la agencia. A menudo se descuida este aspecto. Por ejemplo, las agencias guardan suministros de bajo costo tales como diskettes, en tanto que los activos cibernéticos esenciales, tales como los servidores, quedan sin protección en un área de oficina abierta, y los cables y centros de la red se instalan al descubierto sobre las paredes en lugar de encerrarlos en conductos o esconderlos dentro de los cielos rasos.

También hay que dividir en compartimientos a los usuarios. Controlar las aplicaciones y la información a que tienen acceso y cómo pueden llegar hasta ellas. (Por ejemplo, a un usuario se le puede permitir acceso a ciertas estaciones de trabajo en ciertas ocasiones). Controlar quién puede abrir cuentas o crear identificaciones de usuarios en un sistema. Auditar las cuentas con frecuencia en busca de identificaciones o cuentas que no correspondan a la realidad. Tener a mano personas capaces de llevar a cabo una auditoría.

Una de las amenazas a la seguridad que se descuida con más frecuencia se relaciona con la documentación del sistema. A menudo, la documentación de cualquier tipo se trata con demasiado descuido y es posible encontrarla en oficinas que no son seguras. Hay que proteger la información técnica detallada y la que corresponde a los usuarios. Puede parecer conveniente y menos costoso preparar

documentación que se adapte a todos los usos, pero esto puede resultar peligroso para la seguridad de un sistema. Los manuales de usuario que se distribuyen profusamente contienen a menudo grandes cantidades de información técnica que no le sirve de nada al usuario instalado frente a su terminal, pero que puede ser muy valiosa para el intruso cibernético. Uno de éstos, armado de información detallada sobre el sistema, puede atacarlo con precisión quirúrgica en lugar de apelar a la fuerza bruta, más fácil de detectar. Conviene distribuir la documentación según la necesidad que cada cual tenga de conocerla.

Debe asegurarse la documentación, controlar el acceso a ella y adiestrar a los usuarios acerca de cómo protegerla. Es recomendable, para reducir costos, simplificar la puesta al día y brindar más protección, publicar la documentación en la red en lugar de imprimirla.

6. SEA REALISTA ACERCA DE LA ADMINISTRACION DE LA SEGURIDAD. No es probable que las agencias de justicia penal, por ejemplo, puedan establecer o administrar un programa de seguridad de TI impenetrable. Hay que equilibrar las necesidades de seguridad reales y sus costos. Puede ser posible alcanzar el nivel deseado de apoyo para llegar a las mismasmetas. Puede emplearse personal de la propia agencia para que haga lo que puede hacer efectiva y realísticamente, y recurrir a fuentes externas para el resto. La clave es alcanzar los resultados definidos por el plan de seguridad de la información.

Para satisfacer las necesidades de seguridad, hay disponibles muchos recursos. Pueden obtenerse de una compañía privada a costos competitivos. A medida que aumenta la dependencia de la TI y la seguridad llega a ser una preocupación importante, las empresas responden ofreciendo servicios de seguridad de TI de alta calidad.

También es valioso compartir recursos. Esto incluye lo que las agencias de justicia penal y los miembros de la comunidad de seguridad pueden hacer por cada uno de los otros. Compartir recursos, aportar dinero para hacer compras conjuntas, los servicios que donan las universidades o la comunidad, todas son maneras potenciales de cerrar brechas en el plan de seguridad.

7. PRUEBE, AUDITE, INSPECCIONE SITIOS E INVESTIGUE CONTINUAMENTE Y AL AZAR. Use una metodología para examinar y probar códigos para bloquear las puertas traseras de los sistemas. Use auditoría automática y programas de vigilancia. Use programas para verificar cambios en un documento. Desarrolle y use programas “Tip” como un modo de identificar atacantes reales o potenciales. Dé a conocer las amenazas y las respuestas que se les da. Emprenda siempre acción rápida, constante y apropiada cuando se detectan o informan violaciones. Anuncie con amplitud las medidas disciplinarias tomadas en casos que tengan que ver con la seguridad de la TI.

TECNOLOGIAS EMERGENTES

La seguridad de la TI ha adelantado tan rápidamente como cualquiera de sus otros aspectos, pero no puede ser efectiva si no se la aplica apropiadamente. La aplicación de casi cualquier dispositivo de seguridad está disponible en el comercio. Los cortafuegos son más poderosos y adaptables que nunca y su precio es muy razonable. Los programas de codificación se vuelven más poderosos y fáciles de poner en práctica y mantener. La capacidad de administrar y vigilar sistemas distribuidos desde un punto único de la red mejora constantemente. Los programas de vigilancia y auditoría automáticos para controlar el uso de sistemas y alertar a los administradores de seguridad de intentos de abuso evolucionan con rapidez.

Uno de los aspectos del avance técnico que es más promisorio es la biométrica — la capacidad de identificar a alguien de acuerdo con una característica física exclusiva (por ejemplo, las huellas dactilares, la voz, el contorno de la mano, el patrón retinal, etc.). Los aparatos biométricos hacen posible autenticar a los usuarios con más facilidad que nunca e impedirán que las personas no autorizadas tengan acceso a un sistema, aun si poseen una contraseña.

La IBM, en cooperación con el Barclays Bank en Europa, ensaya teclados que tienen incorporado un lector de huellas dactilares. Los usuarios deben ser autenticados biométricamente antes de que se les permita entrar en cualquier parte del sistema. La tecnología de flash (una búsqueda algorítmica de imágenes) es rápida y precisa. Puede buscar en un banco de datos de

millones de registros (inclusive imágenes de huellas dactilares) para determinar si hay alguno comparable. Esta capacidad, combinada con las redes de alta velocidad, tiene un gran potencial de utilización en los cajeros bancarios automáticos y otros aparatos de transacciones electrónicas. La tecnología de flash se usa en Perú en un sistema de verificación de votantes

basado en las huellas dactilares. El proyecto ha dado resultados excelentes y ayudará a impedir el fraude electoral.

A medida que estas tecnologías evolucionan, la seguridad de la TI seguirá mejorando en términos de efectividad y facilidad de empleo.

LA GUERRA INFORMATICA: DESAFIO Y OPORTUNIDAD

Por James Adams
Director de Infraestructura Defense, Inc.

(“Tengo el poder, la capacidad, sentado en mi hogar con mi computadora y mi módem... de librar una guerra”, dice James Adams. “Ese es un ambiente muy diferente de todo lo que hemos experimentado en el pasado”. Adams es director de Infraestructura Defense, Inc., que ofrece un foro para el intercambio de información y toma de decisiones sobre la infraestructura crítica dentro del sector privado y entre los sectores público y privado en todo el mundo. Este artículo ha sido adaptado de comentarios que hizo Adams en el Servicio Informativo y Cultural de Estados Unidos en agosto de 1998). (“Tengo el poder, la capacidad, sentado en mi hogar con mi computadora y mi módem... de librar una guerra”, dice James Adams. “Ese es un ambiente muy diferente de todo lo que hemos experimentado en el pasado”. Adams es director de Infraestructura Defense, Inc., que ofrece un foro para el intercambio de información y toma de decisiones sobre la infraestructura crítica dentro del sector privado y entre los sectores público y privado en todo el mundo. Este artículo ha sido adaptado de comentarios que hizo Adams en el Servicio Informativo y Cultural de Estados Unidos en agosto de 1998).

Las fuerzas armadas de Estados Unidos organizaron el año pasado un ejercicio que incluía un simulacro en el cual se incubaba una crisis y un gobierno extranjero había contratado a 35 intrusos cibernéticos para trastornar la respuesta estadounidense a esa crisis. Los “intrusos cibernéticos” que participaron en el ejercicio — llamado “Eligible Receiver” — eran, en realidad, empleados del gobierno estadounidense. No se les suministró información de inteligencia por adelantado. Compraron sus computadoras portátiles en un comercio local.

Los intrusos cibernéticos demostraron con éxito que podían penetrar fácilmente las redes de distribución de electricidad de todas las ciudades principales de Estados Unidos — desde Los Angeles a Chicago y desde Washington a Nueva York — que estaban vinculadas con la capacidad estadounidense de despliegue de fuerzas. Al mismo tiempo, pudieron penetrar el sistema telefónico de emergencia “911” y con toda comodidad podrían haber paralizado ambas redes.

Luego pasaron al sistema de comando y control del Pentágono. En el curso de unos pocos días probaron 40.000 redes y consiguieron penetrar 36 de ellas a nivel básico. Lograron penetrar bien adentro de la estructura de comando y control y,

si lo hubieran querido, podrían haber impedido que esa estructura funcionara con eficiencia.

Lo que demostró este ejercicio fue que 35 personas que usaran información disponible públicamente, con destrezas que se pueden conseguir en todo el mundo, realmente podrían haber impedido que Estados Unidos respondiera a una crisis.

Esa es una demostración extraordinaria del poder que representa la guerra informática. Ese poder ha impulsado a Estados Unidos a invertir grandes cantidades de dinero en el desarrollo de una capacidad ofensiva eficaz en la que la guerra se pueda librar por otros medios.

Para quienes tienen la capacidad, existe la oportunidad de librar una guerra — sin desplegar soldados en un sentido común y corriente en un campo de batalla, con la muerte de muchos de ellos, o en efecto, desplegando incluso misiles en la manera usual —, sino, en cambio, lanzando a través del espacio cibernético circuitos integrados que pueden destruir eficazmente a un agresor potencial antes de que las tropas se enfrenten unas a otras en el campo de batalla.

Esto significa apagar las luces en una ciudad importante. Significa impedir que el mercado de

valores funcione de manera apropiada. Significa interrumpir el flujo de información en otro país e insertar el flujo de información propio para hacer posible que se desarrollen operaciones psicológicas muy eficaces contra el enemigo potencial.

Estas cosas suenan bastante simples, pero en realidad pueden causar la clase de pérdidas de vidas que se podría conseguir igualmente con una campaña de bombardeo en gran escala.

Por ejemplo, un estudio de la Fuerza Aérea sobre las consecuencias de capturar la red de distribución de electricidad del sudoeste de Estados Unidos mostró que podrían haber muerto 20.000 personas. Eso habría tenido un efecto devastador en la moral del país y habría presentado interesantes y nuevos desafíos a nuestra manera de responder.

En la crisis con Irak hace pocos meses, a medida que nos dirigíamos hacia posibles acciones militares, se detectó un esfuerzo para interferir con la red logística estadounidense. El origen de esa acción fue eventualmente rastreado a un edificio en Abu Dhabi. Se supuso que esto era el gobernante iraquí Saddam Hussein que libraba una guerra informática contra Estados Unidos en anticipación a la acción militar. Los estadounidenses estaban desplegados para hacer frente a esta amenaza. Después que llegaron al edificio en cuestión, descubrieron un desvío o punto de transferencia en la Internet y que, en realidad, el "ataque" lo habían lanzado unos adolescentes en Estados Unidos.

Esa es una ilustración absoluta del desafío y la oportunidad reales que representa la guerra informática. Podemos lanzar un ataque, y puede parecer que provenga de un lugar muy alejado de su verdadero punto de origen. De la misma manera, cuando inician un ataque contra nosotros, es sumamente difícil descubrir de donde proviene. Incluso si se descubre el origen, es muy difícil lanzar un contraataque. ¿Qué se va a atacar y por qué? ¿Qué respuesta pública y cuanto apoyo público habrá para las acciones que se emprenden si mueren miles de personas? ¿Cómo se persuade a la gente de que esta fue la acción correcta? No hay pruebas que permitan

hablar de bebés muertos que yacen en la calle. No hay un hombre parado en la esquina con un revólver en la mano. No es la clase de cosa a la que está acostumbrada la gente. Esto presenta un verdadero desafío.

Estas cuestiones y las oportunidades que representan resultan muy atractivas para casi cada país que tiene capacidad de operaciones de información. Para el estado nacional el potencial de guerra informática es algo atractivo, pero al mismo tiempo extremadamente amenazante, porque la guerra informática no se depende de las naciones, sino del poder que se le da a los individuos.

Creo que la guerra informática va cambiando fundamentalmente una dinámica que ha existido durante mucho tiempo y que ha ayudado a sostener la estabilidad entre los estados, y consiste en que el gobierno decide el ritmo del cambio, en gran parte, y en que es el instrumento de mucho del cambio.

Cuando se desarrolla un nuevo sistema de armas, pasa bastante tiempo antes que ese sistema de armas llegue desde el país que lo generó hasta un país que no tiene la capacidad de producirlo. Estamos hablando de un ciclo de 20 años. Hoy la computadora más moderna la produce Compaq, los programas son de Microsoft, y se venden en CompUSA, una tienda de computadoras con locales en todo Estados Unidos. Quizás, sólo quizás, el gobierno pueda comprarla dentro de dos o tres años, pero es improbable. Mientras que yo puedo ir a la tienda de computadoras con mi chequera en la mano y comprarla. En una guerra informática, esa es mi arma.

Tengo el poder, la capacidad, sentado en mi hogar con mi computadora y mi módem, de librar una guerra... si sólo comprendiera cómo hacerlo. Ese es un ambiente muy diferente de todo lo que hemos experimentado en el pasado.

Creo que algo particularmente interesante que estamos observando a medida que se desarrolla la revolución de la información —y apenas estamos en sus comienzos— es la nueva gama de alianzas que están surgiendo. Recientemente

hablé con un amigo que había coordinado una conferencia en línea de montañeses. Se trata de gente que vive en las montañas de todo el mundo — en los Alpes, los Urales, las Montañas Rocosas o donde sea — y tuvieron una conferencia en línea de dos días. Esta gente, que nunca se había comunicado antes, se enteró de que tiene muchas cosas en común. Todos ellos detestan a la gente de los valles. Todos ellos detestan al gobierno y todos ellos se preocupan apasionadamente por el medio ambiente.

Ese es un ejemplo de una nueva comunidad cuyos miembros tienen más cosas en común entre sí, quizás, que con los otros ciudadanos de las naciones en las cuales viven. Ahora esos grupos — ya sean 52 organizaciones terroristas que tienen actualmente lugares en la web, organizaciones ambientalistas o gente que simplemente se siente privada de sus derechos — tienen todos la capacidad de comunicarse entre ellos, de compartir conocimiento, de expresar sus frustraciones. Es asombrosa la capacidad de unión que hay entre estos grupos, que nunca había existido antes.

Aunque no tenemos la capacidad de eliminar la probabilidad de una guerra, tenemos la capacidad ofensiva para librar la guerra por otros medios y ciertamente cambiar la manera en que nos encaminamos hacia el conflicto tradicional. Y eso presenta algunos desafíos reales. Antes que nada, el gobierno tiene que comprender lo que significa la guerra. Todavía estamos encerrados en un ambiente de la guerra fría. Si se le pregunta a la Fuerza Aérea, a la Armada o a los otros que están desarrollando estas capacidades, “cuándo se les permitirá usar lo que tienen”, responden: “Bien, le hemos hecho esa pregunta al Departamento de Justicia hace un par de años y no nos han respondido todavía”.

Ese es un asunto importante. Estas armas están diseñadas para ser usadas exactamente antes de que vayamos a la guerra para prevenir que lo hagamos en el sentido tradicional. Y, sin embargo, son muy agresivas y muy poderosas. Ese desafío va a ser muy grande para el gobierno. Ya lo es. ¿Cómo sigue teniendo importancia el gobierno cuando todo alrededor suyo cambia con tanta velocidad?

Nosotros también, en una manera defensiva, tenemos que tratar con un tipo diferente de amenaza. Tradicionalmente, los militares se han visto a ellos mismos como soldados que van al frente de combate, pelean, caen heridos, mueren o regresan; tienen éxito o fracasan. Pero en el nuevo ambiente, todos nosotros estamos ahora en la línea del frente. La cuestión es cómo nos defendemos y protegemos así como nos protege el gobierno o el sector privado. Somos parte del proceso. Esto representa un ambiente muy diferente.

El problema del año 2000 (Y2K) es una muy buena ilustración de esto. En realidad es una cuestión social, de la misma manera en que la guerra informática es una cuestión social. La guerra informática consiste en cortar el agua, cortar la electricidad, trastornar el funcionamiento de las plantas de tratamiento de aguas servidas y paralizar los sistemas de ATM (cajeros bancarios automáticos), despedazando el tejido de la vida.

Tratar con el problema del Y2K va a demostrar la amplitud de la interdependencia de las infraestructuras esenciales. Ninguno de nosotros comprende todavía completamente cuán interconectado está todo lo que hacemos. Si se cae una pieza, también se rompe el resto del rompecabezas. No se trata sólo de una cuestión nacional, es un asunto internacional.

De manera que a medida que avanzamos para atender los desafíos de la guerra informática, tenemos que atender al mismo tiempo los desafíos del gobierno. ¿Qué significa eso en este nuevo ambiente? Tenemos que atender el desafío de la infraestructura esencial. ¿Cómo defendemos eso adecuadamente?

Un elemento vital es el sector privado, porque él es el motor que dirige ahora el cambio que se desarrolla en torno a nosotros. El gobierno tiene que demostrar su importancia y asumir en esto alguna forma de liderazgo, de lo cual creo que está notoriamente ausente.

El sector privado puede articular muchas de estas cosas para defenderse y, por lo tanto, defendernos a cada uno de nosotros. Si no reconocemos eso, creo que tendremos algunos problemas muy graves, empezando con el del Y2K. Seremos víctimas de los nuevos agresores

que hay allí afuera, que tienen un poder que nosotros nunca hemos comenzado a comprender verdaderamente, y cuando lo comprendamos, será demasiado tarde.

Lo que yo propondría es tratar de educar a la gente con respecto a estos temas y alentar nosolamente el conocimiento público sino también más acción por parte de quienes tienen la capacidad de difundir la palabra y, por lo tanto, crear defensas contra lo que va a ser un ambiente extremadamente agresivo en el próximo siglo.

HOJA INFORMATIVA: LA PROTECCION DE LAS INFRAESTRUCTURAS ESENCIALES DE ESTADOS UNIDOS

(Directiva de Decisión Presidencial 63)

(La siguiente hoja informativa sobre la Directiva de Decisión Presidencial 63 fue dada a luz pública por la Casa Blanca el 22 de mayo de 1998).

La presente Directiva de Decisión Presidencial se fundamenta en las recomendaciones de la Comisión Presidencial sobre la Protección de las Infraestructuras Esenciales. En octubre de 1997, la comisión emitió un informe en el que hacía un llamado a un esfuerzo nacional para garantizar la seguridad de las cada vez más vulnerables infraestructuras interconectadas de Estados Unidos, como son las telecomunicaciones, la banca y finanzas, la energía eléctrica, el transporte y los servicios esenciales del gobierno.

La Directiva de Decisión Presidencial 63 es la culminación de un laborioso esfuerzo realizado por los diferentes organismos de gobierno con el fin de evaluar esas recomendaciones y producir un marco de trabajo innovador para proteger las infraestructuras esenciales. La política del presidente:

— Establece como objetivo una infraestructura del sistema informático que sea fiable, interconectada y segura para el año 2003, y una mayor y significativa seguridad de los sistemas de gobierno para el año 2000, para lo cual:

a) Establecerá inmediatamente un centro nacional para advertir sobre ataques y responder a ellos.

b) Establecerá la capacidad de proteger las infraestructuras esenciales contra actos deliberados para el año 2003.

— Aborda la vulnerabilidad de la infraestructura informática y física del gobierno federal, por lo cual requiere a cada departamento y organismo que aminore el riesgo de nuevas amenazas;

— Requiere del gobierno federal que sea modelo para el país sobre cómo lograr la protección de la infraestructura;

— Pretende obtener la participación voluntaria de la industria privada para lograr los objetivos comunes de la protección de nuestros sistemas esenciales por medio de asociaciones públicas-privadas;

— Protege derechos de confidencialidad y pretenden utilizar la fuerzas del mercado. Tiene como fin consolidar y proteger el poder económico del país, y no contenerlo.

— Pretende la participación y aporte del Congreso.

La Directiva de Decisión Presidencial 63 establece una nueva estructura para afrontar este importante reto:

— Un Coordinador Nacional en cuya esfera de trabajo se incluye no sólo a las infraestructuras esenciales, sino también al terrorismo del extranjero y las amenazas de destrucción en masa del país (con inclusión de armas biológicas), porque los ataques a Estados Unidos no vienen con etiquetas que establecen sus características o destino;

— El Centro de Protección de Infraestructuras Nacionales en la Oficina Federal de Investigaciones (FBI), que utilizará los servicios de representantes del FBI, del Departamento de Defensa, del Servicio Secreto de Estados Unidos, de los departamentos de Asuntos Energéticos y del Transporte, de la comunidad de Servicios de Inteligencia y el sector privado en un intento sin

precedente por compartir información entre los organismos de gobierno con la colaboración del sector privado. El Centro también proporcionará los principales medios para facilitar y coordinar la respuesta del gobierno federal a un incidente, mitigar un ataque, investigar amenazas y hacer seguimiento de los esfuerzos de reconstitución;

— Un Centro de Intercambio y Análisis, que se alienta establezca el sector privado con la cooperación del gobierno federal;

— Un Consejo de Seguridad de las Infraestructuras Nacionales constituido por líderes del sector privado y funcionarios del gobierno estatal y local para proporcionar orientación en la formulación de normas de política de un Plan Nacional;

— Una Oficina de Seguridad de Infraestructuras Esenciales para proporcionar apoyo a la labor del Coordinador Nacional con los organismos de gobierno y el sector privado en la elaboración de un plan nacional. La oficina también ayudará a coordinar un programa de educación y concientización de la nación, así como asuntos públicos y legislativos.

Para más información sobre la Directiva de Decisión Presidencial, comuníquese con la oficina de Critical Infrastructure Assurance llamando al (703) 696-9395 para obtener ejemplares del informe titulado “White Paper on Critical Infrastructure Protection” (Informe Oficial sobre Protección de Infraestructuras Esenciales).

LA AMENAZA CIBERNETICA ALERTA SOBRE ARTICULOS (en inglés)

(en inglés)
(Extractos de artículos actuales)

Bennett, Robert, et al. THE Y2K CRISIS: A GLOBAL TICKING TIME BOMB? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 147-166)

Management consultants, financial planners, and experts in year 2000 conversion issues warn, in five essays, that the Y2K computer problem deserves to be taken seriously — and soon, before it is too late. Senator Bennett, who chairs a Senate Special Committee on the Y2K problem, says the “biggest challenge” is “to get people thinking...across the individual lines of our own organizations, indeed across the individual lines of our own country’s borders.” And “we must...recognize that this is not an IT (information technology) problem” but rather “a management challenge” that must be addressed immediately at the highest levels, he says.

Bowers, Stephen R. INFORMATION WARFARE: THE COMPUTER REVOLUTION IS ALTERING HOW FUTURE WARS WILL BE CONDUCTED (Armed Forces Journal International, August 1998, pp. 38-39)

Contending that access to information today is just as crucial as possession of petroleum and ammunition, Bowers discusses the threat posed by “almost invisible computer assailants” to a nation’s power grids, transportation networks, financial systems, and telephone exchanges. He says recent U.S. military exercises have involved actions that elevate IW (information warfare) from a tactical to a strategic level. IW involves a new kind of battlefield but with the potential for equally as many casualties, he says.

Gompert, David C. NATIONAL SECURITY IN THE INFORMATION AGE (Naval War College Review, vol. 51, no. 4, sequence 364, Autumn 1998, pp. 22-41)

Gompert, director of the National Defense Research Institute at RAND, argues that the changes brought about by the information revolution, though not without drawbacks, have greatly benefited the United States. The information revolution has extended economic and political freedom, Gompert states, expanding the world’s “democratic core.” It has brought about significant changes in the conduct of warfare, giving the United States, with its lead in information technology, a great advantage: “Roughly stated, information technology can help those who master it to win large wars at long distances with small forces,” says Gompert. He cites a concern that rogue states “are likely to turn to asymmetric strategies, for instance, weapons of mass destruction, terrorism, and information warfare (IW) attacks against the United States and its partners.”

Henry, Ryan; Peartree, C. Edward. MILITARY THEORY AND INFORMATION WARFARE (Parameters, vol. 28, no. 3, Autumn 1998, pp. 121-135)

The authors examine the limited influence that technologies have had on warfare and cite as an example the airplane, which, though adding an unprecedented technological breakthrough to the battle space, repeatedly has been shown to be insufficient in and of itself to transform war. Old weapons do not necessarily go out of style — “new tools are just added to the box,” the authors say. Underscoring the importance of grasping “the functional significance of technological innovations,” they contend “it is equally important that risks and vulnerabilities — the stuff of strategy — remain foremost in assessing their political and military implications. The most durable military theory focuses less on the latest technology and more on the infinite complexity of the user.”

Selden, Zachary. MICROCHIPS AND THE MILLENNIUM: THE NATIONAL SECURITY IMPLICATIONS OF THE YEAR 2000 PROBLEM (National Security Studies Quarterly, vol. 4, issue 3, Summer 1998, pp. 71-77)

Selden predicts that most computer software associated with the year 2000 problem will be fixed or discarded and that most of the problematic embedded computer chips will be replaced by January 1, 2000. What remains could cause unpredictable failures or sow confusion sufficient to allow states or terrorists to conduct covert disruptions or intrusions, he says. International

actors may seek “to take advantage of a distracted United States” at the turn of the millennium, the author warns, and some current regional flash points might erupt “into a spiral of conflict because of failed systems.” From a national security perspective the problem “is the perception that Y2K presents a window of vulnerability,” the author says.

The annotations above are part of a more comprehensive Article Alert offered on the home page of the U.S. Information Service:
“<http://www.usia.gov/admin/001/wwwhapub.html>”.

LA AMENAZA CIBERNETICA

BIBLIOGRAFIA (en inglés)

(en inglés)

(Destaca otras opiniones sobre el tema)

Adams, James. THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE. New York: Simon & Schuster, 1998. 366p.

Arquilla, John; Ronfeldt, David F. (Editors). IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE. Santa Monica, CA: Rand, 1997. 501p.

Barnett, Roger W. INFORMATION OPERATIONS, DETERRENCE, AND THE USE OF FORCE (Naval War College Review, vol. 51, no. 2, Spring 1998, pp. 7-19)

Browne, J.P.R.; Thurbon, M.T. ELECTRONIC WARFARE, Vol. 4 of Brassey's Air Power: Aircraft Weapons Systems and Technology Series. Washington: Brassey's, 1998. 341p.

Cillufo, Frank J.; Tomarchio, Thomas. RESPONDING TO NEW TERRORIST THREATS (Orbis, vol. 42, no. 3, Summer 1998, pp. 439-452)

Clinton, William J. COMMENCEMENT ADDRESS AT THE UNITED STATES NAVAL ACADEMY IN ANNAPOLIS, MARYLAND (Weekly Compilation of Presidential Documents, vol. 34, no. 21, May 22, 1998, pp. 944-948)

Copley, Gregory R. RE-DEFINING PSYCHOLOGICAL STRATEGY IN THE AGE OF INFORMATION WARFARE (Defense & Foreign Affairs Strategic Policy, vol. 26, no. 6, June 1998, pp. 5-8)

Gunther, Christopher. YOU CALL THIS A REVOLUTION? (Foreign Service Journal, vol. 75, no. 9, September 1998, pp. 18-23)

Henry, Ryan; Peartree, C. Edward (Editors). INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Significant Issues Series, vol. 20, no. 1). Washington: Center for Strategic & International Studies, 1998. 216p.

Libicki, Martin C. INFORMATION WAR, INFORMATION PEACE (Journal of International Affairs, vol. 51, no. 2, Spring 1998, pp. 411-428)

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR. Santa Monica, CA: Rand, 1996. 90p.

Petersen, John L.; Wheatley, Margaret; Kellner-Rogers, Myron. THE YEAR 2000: SOCIAL CHAOS OR SOCIAL TRANSFORMATION? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 129-146)

Pfaltzgraff, Robert L.; Schultz, Richard H. (Editors). WAR IN THE INFORMATION AGE: NEW CHALLENGE FOR U.S. SECURITY POLICY. Washington: Brassey's, 1997. 320p.

Rathmell, Andrew. INFORMATION WARFARE: USA TACKLES CYBERTHREAT (Jane's Intelligence Review Pointer, vol. 5, no. 9, September 1, 1998, p. 14)

Ryan, Stephen M. SHOULD U.S. PLEDGE NOT TO MAKE FIRST CYBERSTRIKE? (Government Computer News, vol. 17, no. 24, August 3, 1998, p. 32)

Sanz, Timothy L. INFORMATION-AGE WARFARE: A WORKING BIBLIOGRAPHY (Military Review, vol. 78, no. 2, March-April 1998, pp. 83-90)

U.S. Senate, Select Committee on Intelligence. CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES. Washington: Government Printing Office, 1998. 177p.

Verton, Daniel. DOD PREPS OFFICE FOR CYBERDEFENSE (Federal Computer Week, vol. 12, no. 23, July 13, 1998, pp. 1-2)

LA AMENAZA CIBERNETICA

SITIOS CLAVES EN LA INTERNET (en inglés)

Please note that USIS assumes no responsibility for the content and availability of the resources listed below; such responsibility resides solely with the providers.

Air Force Information Warfare Center
<http://www.afiwcenter.af.mil/>

Center for High Assurance Computer Systems of the Naval Research Laboratory
<http://www.itd.nrl.navy.mil/ITD/5540/main.html>

Computer Security Technology Center, Lawrence Livermore National Laboratory, U.S. Department of Energy
<http://ciac.llnl.gov/cstc/>

Critical Infrastructure Assurance Office
<http://www.ciao.gov/>

Cyberspace Policy Institute at George Washington University
<http://www.seas.gwu.edu/seas/institutes/cpi/>

Defense Information Infrastructure
<http://spider.osfl.disa.mil/dii/>

Defense Policy on the Year 2000 Computer Conversion Issue
<http://www.defenselink.mil/issues/y2k.html>

Glossary of Information Warfare Terms
<http://www.psycom.net/iwar.2.html>

IBM Corporation: Secure Way
<http://www.ibm.com/Security/>

Information Systems Security Association
<http://www.issa-intl.org/>

Information Warfare Academic Group, Naval Postgraduate School
<http://web.nps.navy.mil/~iwag/>

Information Warfare and Information Security on the Web
<http://www.fas.org/irp/wwwinfo.html>

Information Warfare: Glossary
<http://www.informatik.umu.se/%7Erwhit/IWGlossary.html>

Information Warfare Research Center
<http://www.terrorism.com/infowar/documents.html>

InfoWar.Com
<http://www.infowar.com/main.html>

Infrastructure Defense, Inc.
<http://206.132.10.154/idmarketsite/>

Microsoft Corporation (Key Initiatives)
<http://www.microsoft.com/>

National Colloquium for Information Systems Security
<http://www.infosec.jmu.edu/ncisse/>

National Infrastructure Protection Center of the Federal Bureau of Investigation
<http://www.fbi.gov/nipc/home.htm>

National Institute of Standards and Technology (NIST)
<http://csrc.nist.gov/>

National Security Agency
<http://www.nsa.gov:8080/>

President's Council on Year 2000 Conversion
<http://www.Y2K.gov/java/index.htm>

School of Information Warfare and Strategy,
National Defense University
<http://www.ndu.edu/inss/act/iwscvr.html>

Technology News: Governments Beat Terrorists
To Net Weapons
[http://www.techweb.com:80/wire/story/
TWB19980922S0018](http://www.techweb.com:80/wire/story/TWB19980922S0018)

U.S. Senate, Committee on the Judiciary,
Subcommittee on Technology, Terrorism, and
Government Information
<http://www.senate.gov/~judiciary/terrtest.htm>

Year 2000 Conversion: U.S. Information Agency
<http://www.usia.gov/topical/global/y2k/>



USIS

Servicio Cultural e Informativo de los Estados Unidos