Aseguramiento de infraestructuras y

Jeffrey F. Addicott*
Director del Centro de Derecho Terrorista, St Mary´s University

I. Introducción

Mientras algunos trazan el inicio de la Guerra contra el Terrorismo al 11 de septiembre de 2001, es claro hoy en día que Estados Unidos ha sido el principal blanco de los ataques terroristas por grupos islámicos radicales durante muchos años. La Comisión Nacional de Ataques Terroristas contra Estados Unidos (Comisión 9/11) afirmó que la Inteligencia Americana y las agencias de orden público sufrieron "una falta de imaginación".[1] El gobierno sencillamente no tomó en serio la posibilidad de que terroristas utilizaran aerolíneas comerciales como armas de precisión para atacar edificios. La falla en apreciar la sofisticación de

1 La Comisión Nacional de Ataques Terroristas contra Estados Unidos se cerró el 21 de agosto de 2004.

* El autor desea expresar su gratitud a Jordan Linscomb por su excelente asistencia en la investigación.

"Desde los ataques del 11 de septiembre de 2001, el gobierno ha creado una variedad de respuestas antiterroristas robustas diseñadas para socavar las redes terroristas y reducir la posibilidad de ataques futuros de esta índole. Incluyendo la aprobación de la *Ley Patriota*, la creación del cargo de nivel de gabinete de Seguridad del Territorio Nacional y el establecimiento del Comando Norte de Estados Unidos en Colorado, la primera nación del mundo también ha participado en otras acciones tales como el uso preventivo de fuerza militar contra Estados deshonestos, para incluir a aquellos que apoyan o patrocinan terrorismo del estilo Al-Qaeda y la detención indefinida de presuntos terroristas extranjeros ilegales y combatientes del enemigo".

la red terrorista Al-Qaeda[2] abrió la puerta a los devastadores ataques. Como consecuencia, Estados Unidos fue tomado completamente por sorpresa resultando en la pérdida de más de 3.000 vidas y miles de millones en propiedades.[3]

Desde los ataques del 11 de septiembre de 2001, el gobierno ha creado una variedad de respuestas antiterroristas robustas diseñadas para socavar las redes terroristas y reducir la posibilidad de ataques futuros de esta índole.[4] Incluyendo la aprobación de la *Ley Patriota*[5], la creación del cargo de nivel de gabinete de Seguridad del Territorio Nacional[6] y el establecimiento del Comando Norte de Estados Unidos en Colorado[7], la primera nación del mundo también ha participado en otras acciones tales como el uso preventivo de fuerza militar contra Estados deshonestos, para incluir a aquellos que apoyan o patrocinan terrorismo del estilo Al-Qaeda y la detención indefinida de presuntos terroristas extranjeros ilegales y combatientes del enemigo.

ciberterrorismo

2 La organización terrorista Al-Qaeda fue fundada en 1989 por un saudita llamado Osama bin Laden. Dedicada a la destrucción de Occidente, la organización ha demostrado, durante los últimos tres años, que es realmente de alcance internacional con recursos y personal para coordinar ataques terroristas sofisticados en una escala nunca vista. Está ligada a una variedad de grupos terroristas desde Filipinas a Indonesia y ha entrenado a decenas de miles de militantes árabes y no árabes en Afganistán bajo el régimen Talibán. Alimentada por un radicalismo islámico súper fundamentalista, sus soldados de odio gustosamente aceptan la muerte en su búsqueda de muertes masivas. Ver Michael Elliott, Por qué la guerra contra el terror jamás concluirá, Mayo 26, 2003, en 29.

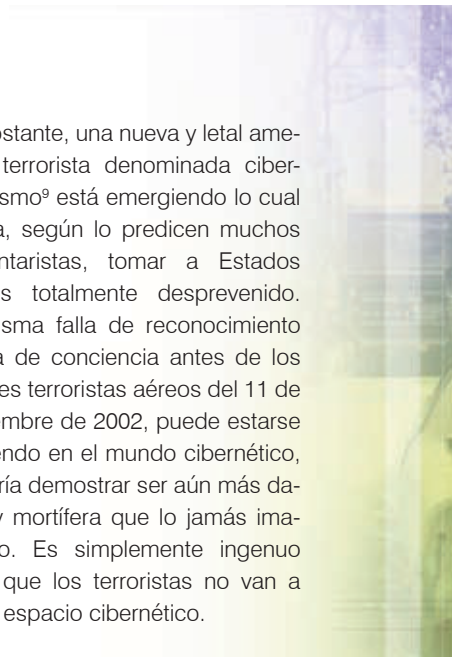
3 Goode, Erica. Un día de terror: la psicología. N.Y. Times, sep.12, 2001, en A13 (en adelante Día de terror). El 11 de septiembre de 2001, un total de 19 miembros de la red terrorista Al-Qaeda secuestraron cuatro aviones de aerolíneas domésticas de EE.UU, estando en vuelo cinco terroristas en los tres aviones, y cuatro en el cuarto). Los terroristas estrellaron dos aviones contra las torres gemelas del World Trade Center en Nueva York. Otro avión fue estrellado contra el Pentágono en Washington, pero, el cuarto avión fue derribado por los pasajeros en un campo en Pennsylvania. Según un análisis de N.Y. Times, junto con miles de millones en propiedades, aproximadamente 3.067 murieron, sin incluir a los terroristas. Esta cifra incluye a 184 muertos en el Pentágono (contando los 59 pasajeros del avión secuestrado) y 40 muertos en Pennsylvania. Ver Muertos y desparecidos, N.Y. Times, 10 de febrero de 2002, en A12, col1.

4 Ver, La Estrategia de Seguridad Nacional de Estados Unidos de América. Casa Blanca, Washington, D.C. 17 de septiembre de 2002, p.15 (en adelante Estrategia de Seguridad Nacional) (la llamada Doctrina Bush adopta el uso de fuerza preventiva en defensa propia y está diseñada para impedir el matrimonio del terrorismo estilo Al-Qaeda con las armas de destrucción masiva).

5 La Ley para unir y fortalecer a Estados Unidos proporcionando las herramientas apropiadas requeridas para interceptar y obstruir al terrorismo de 2001, Pub. L. No. 107-56. 115 Stat. 272 (Octubre 26, 2001). La ley fue aprobada por el Senado por una inmensa mayoría del 98-1. 147 Cong. Rec. S11,059,60 (Octubre 25, 2001). La Cámara de Representantes aprobó su versión por una similar mayoría de 357-66. 147 Cong. Rec. H7224 (Octubre 25, 2001) Ver también, la página web del Centro de Información Privada Electrónica en la Ley Patriota EE.UU.

6 (En adelante Ley de Seguridad del Territorio Nacional); Ver en general Editorial, *Buscando la Seguridad del Territorio Nacional* , New York Post, Junio 7, 2002 en 32 (el departamento de Seguridad del Territorio nacional incorpora a más de 100 diferentes divisiones gubernamentales de ocho departamentos del Gabinete separados en una sola agencia cuya única misión es garantizar la seguridad interna del país).

7 El Comando Norte de EE.UU está ubicado en la Base de la Fuerza Aérea Peterson en Colorado Springs, Colorado. Fue establecido el 1 de octubre de 2002 y es el único cuartel militar enfocado en defensa nacional y en asistir a la Nación después de un gran desastre natural o un ataque por el hombre. Actualmente hay aproximadamente 500 personas militares y civiles asignadas al nuevo comando. Ver Crawley, Vince. 9-11 Medios 24-7 Comando Norte analiza todas las amenazas- causadas por el hombre o por la naturaleza, Army Times, Enero 19, 2003 at 18.



"Hay un creciente cuerpo de evidencia de que un ataque terrorista cibernético ocurra en el país de la primera economía del mundo en el futuro cercano. Cuando se considera que las organizaciones terroristas tales como Al-Qaeda y Hamas han estado utilizando computadores, correo electrónico y encriptación para apoyar y financiar sus organizaciones durante años, es solamente lógico concluir que están plenamente concientes de que el ciberterrorismo ofrece un método de bajo costo para causar grandes daños y es muy difícil de rastrear".

Sin duda alguna, el cambio de enfoque táctico de castigar a individuos, organizaciones o naciones que cometen crímenes terroristas o participan en agresiones[8], precisa de nuevas metodologías amplias, diseñadas a impedir dichos actos criminales y tal hecho, ha causado un mar de cambios en la forma como el gobierno aborda la prevención del terrorismo.

No obstante, una nueva y letal amenaza terrorista denominada ciberterrorismo[9] está emergiendo lo cual podría, según lo predicen muchos comentaristas, tomar a Estados Unidos totalmente desprevenido. La misma falla de reconocimiento y falta de conciencia antes de los ataques terroristas aéreos del 11 de septiembre de 2002, puede estarse repitiendo en el mundo cibernético, y podría demostrar ser aún más dañina y mortífera que lo jamás imaginado. Es simplemente ingenuo creer que los terroristas no van a adaptar sus armas para atacar el espacio cibernético.

El propósito de este artículo es discutir la amenaza del ciberterrorismo y analizar algunas de las nuevas herramientas que Estados Unidos está empleando para confrontar la amenaza. Como se dijo antes, hay un creciente cuerpo de evidencia de que un ataque terrorista cibernético ocurra en el país de la primera economía del mundo en el futuro cercano.[10] Cuando se considera que las organizaciones terroristas tales como Al-Qaeda y Hamas han estado utilizando computadores, correo electrónico y encriptación para apoyar y financiar sus organizaciones durante años, es solamente lógico concluir que están plenamente concientes de que el ciberterrorismo ofrece un método de bajo costo para causar grandes daños y es muy difícil de rastrear.

II. La Amenaza del ciberterrorismo

El mundo moderno que hemos creado depende totalmente del trabajo de Internet, bases de datos de computadoras y software del mundo cibernético. Indudablemente, el reino cibernético está plenamente incorporado en nuestras vidas cotidianas y toca casi todo lo que hacemos o pensamos. Aparte de servir como un medio de comunicación fantástico, el mundo cibernético regula todos los aspectos de nuestra infraestructura para tener agua, electricidad, bancos, transporte, tecnología, agricultura, medicina, instalaciones nucleares, manejo de recibos, servicios estatales, entre otros bienes y servicios. Este hecho no solamente alimenta la era de los crímenes cibernéticos, también ha resultado en el espectro del ciberterrorismo.

El ciberterrorismo es el uso de diversos recursos de informática para intimidar o forzar a otro -generalmente al gobierno- al desarrollo de objetivos específicos. Un comentarista lo ha definido

8 Definición de Agresión, Res. 3314 Asamblea general. La definición de la ONU de agresión, establece en su parte principal:

Artículo 1

Agresión es el uso de fuerza armada por un Estado contra la soberanía, integridad territorial o independencia política de otro Estado, o en cualquier forma inconsistente con la Carta de las Naciones Unidas...

Artículo 2

El primer uso de fuerza armada por un Estado en contravención a la Carta constituirá evidencia *prima facie* de un acto de agresión...

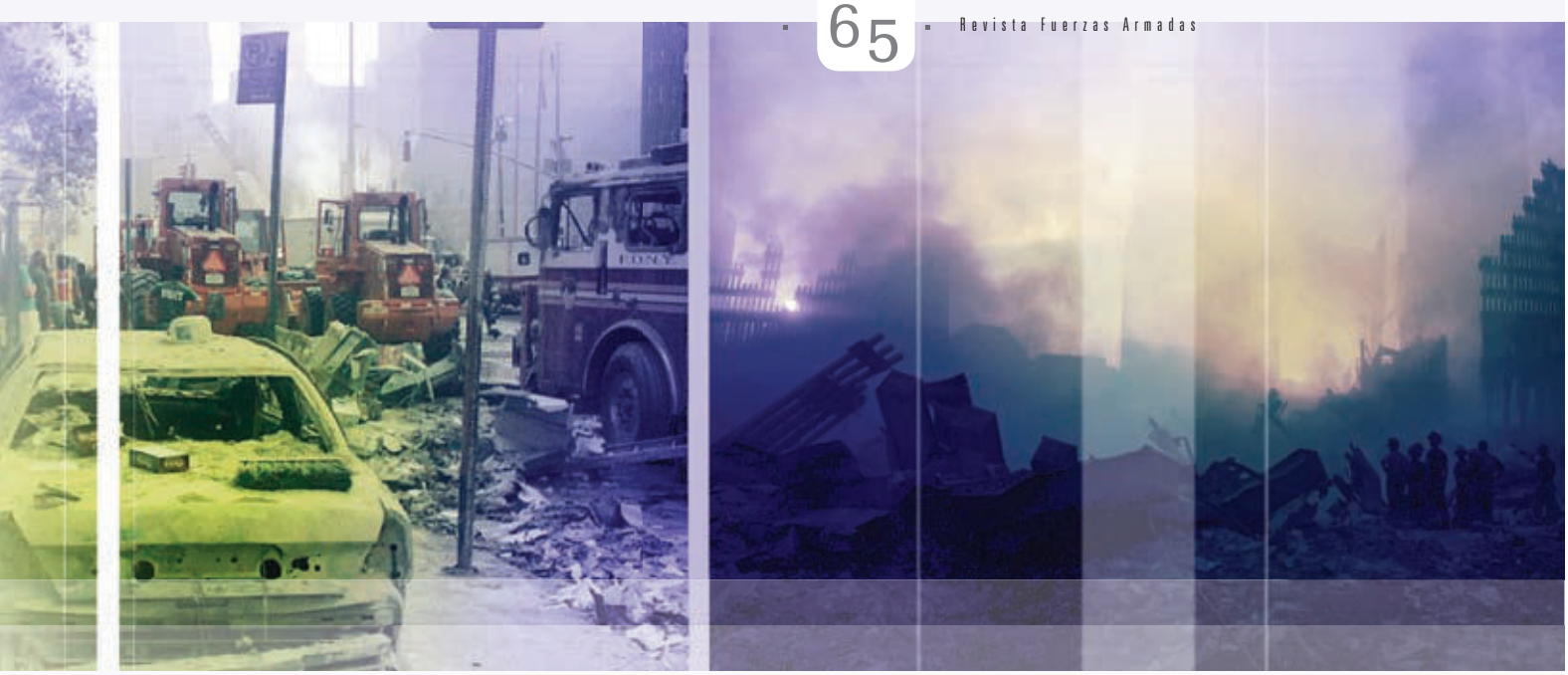
Artículo 3

Cualesquiera de los siguientes actos, no obstante una declaración de guerra, se tendrá.... como un acto de agresión:

a) Invasión o ataque por la Fuerzas Armadas de un Estado... de otro Estado o de una parte del mismo;
b) Bombardeo por parte de las Fuerzas Armadas de un Estado contra el territorio de otro Estado...
c) El bloqueo de puertos o costas de un Estado por las Fuerzas Armadas de otro Estado,
d) Un ataque por las Fuerzas Armadas de un Estado en tierra, mar, Fuerzas Aéreas o flotas aéreas o marítimas de otro Estado,
e) El uso de Fuerzas Armadas de un Estado... en violación de las condiciones establecidas en el acuerdo o cualquier extensión de su presencia en dicho territorio después de terminado el acuerdo,
f) La acción de un Estado en permitir que su territorio que, ha sido puesto a disposición de otro Estado sea utilizado por dicho u otro Estado para cometer actos de agresión contra un tercer Estado, o
g) El envío por o en nombre de un Estado, de bandas, grupos, irregulares, o mercenarios que lleven a cabo actos de fuerza armados contra otro Estado de tal magnitud que se asimila a los actos arriba mencionados, o su importante participación en los mismos.

9 El término ciberterrorismo fue creado por Barry Collin, un alto investigador del Instituto de Seguridad e Inteligencia en California

10 Ver Beth Guard, Mary. Amenazas físicas y digitales a las instituciones financieras en los albores de ataques terroristas. Bankers Online, 2001.



como "*el ataque premeditado, políticamente motivado contra la informática, sistemas de computadoras, programas de computadoras, y datos que resulten en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos*"[11]. Por tanto, el ciberterrorismo involucra actividades para trastornar, corromper, rechazar o destruir información contenida en computadoras o redes de computadoras. Por supuesto, no todos los actos de los crímenes cibernéticos están bajo la definición de ciberterrorismo.

En el léxico de la terminología de informática hay tres tipos de criminales cibernéticos: (1)script-kiddies, (2) hackers, y (3) crackers. Los ciberterroristas pertenecen al grupo de criminales cibernéticos más peligrosos, el cracker. Los script-kiddies son criminales de informática de bajo nivel. Generalmente, descargan diferentes paquetes y herramientas de informática de Internet y los utilizan para explotar las debilidades en seguridad con el objeto de, por ejemplo, desfasar una página web o acosar a ciertos usuarios. El hacker es más sofisticado que el script-kiddie y utiliza sus mayores habilidades en informática para penetrar sistemas seguros, generalmente por la emoción y satisfacción del logro. Entre más seguro sea el sistema penetrado, mayor la emoción. De hecho, en agosto de 2004, el público supo qué hackers habían penetrado cientos de "poderosos computadores del Departamento de Defensa y del Senado de Estados Unidos" y los utilizaron para mandar correos electrónicos spam.[12] Por otra parte, el cracker es el más peligroso cibercriminal. El cracker ataca el sistema de informática para verdaderos propósitos criminales que incluyen chantaje, espionaje o simple malicia, como los creadores de virus. "*Los ciberterroristas se agrupan con los crackers porque comparten los mismos propósitos malévolos....*".[13]

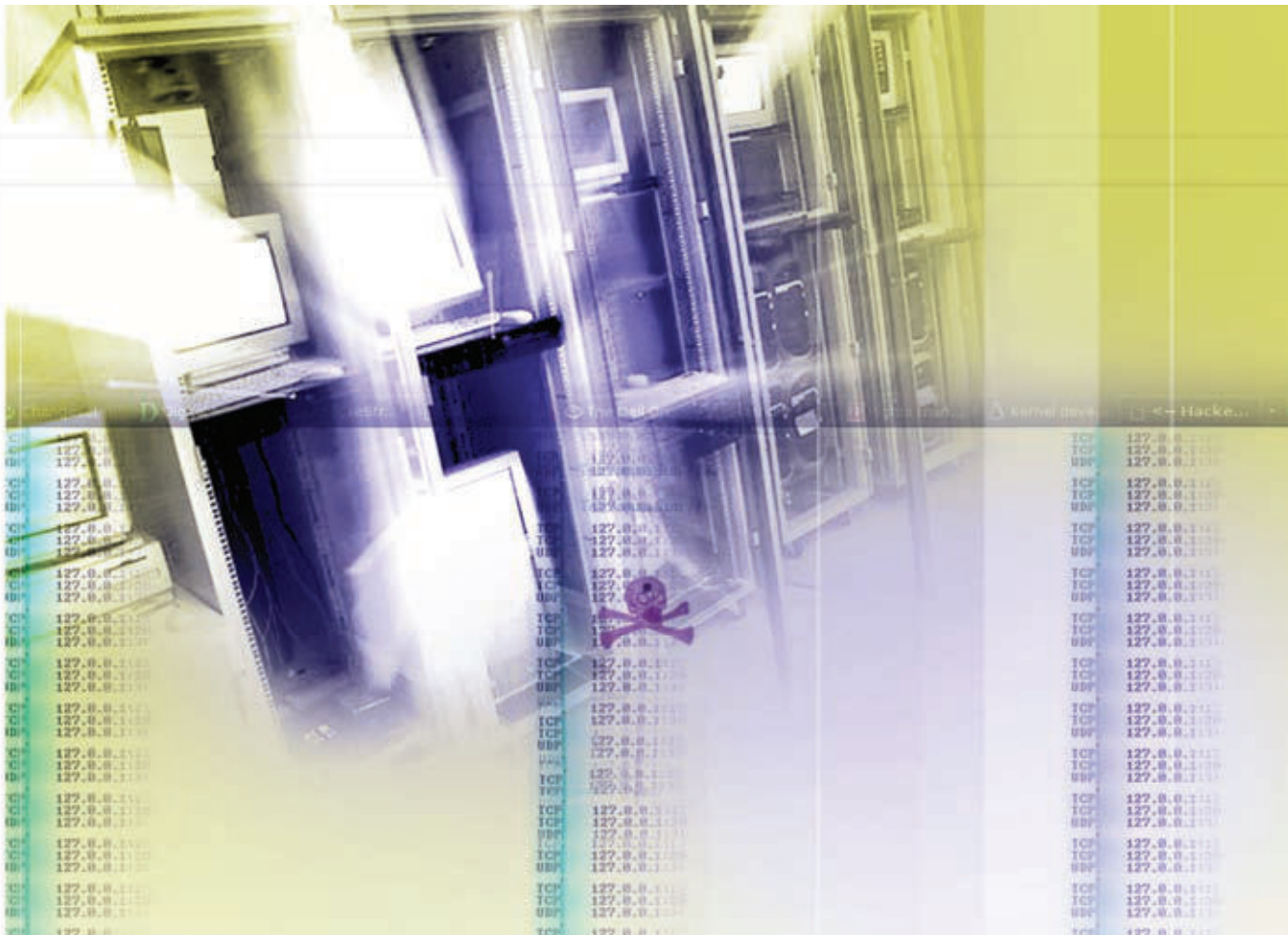
Aquellos no familiarizados con el término ciberterrorismo piensan que el concepto significa atacar Internet. Esto es un punto de vista demasiado simplista. Un ataque cibernético sería utilizado para destruir no solamente la infraestructura electrónica de un país sino también la infraestructura física. Esto es posible porque parte de las infraestructuras más importantes de la nación como los sistemas de defensa, materiales químicos y peligrosos, sistemas de suministro de

"Aquellos no familiarizados con el término ciberterrorismo piensan que el concepto significa atacar Internet. Esto es un punto de vista demasiado simplista. Un ataque cibernético sería utilizado para destruir no solamente la infraestructura electrónica de un país sino también la infraestructura física".

11 Ver Pollit, Mark. Ciberterrorismo: ¿mito o realidad?. October 1997, en 285-289

12 Swarts, Jon. Hackers Secuestran a las computadoras federales. USA Today. Agosto 31, 2004, en 1B

13 Id. en 921



agua, transporte, energía, sistemas financieros, y servicios de emergencia son controlados por redes de computadores centralizadas denominadas Sistemas de Control Supervisor y Adquisición de Datos, SCDA. Los sistemas SCDA proporcionan la "potencial cerebral" para manejar infraestructuras críticas. Un ataque ciberterrorista exitoso contra un solo SCDA podría ocasionar daños económicos y físicos masivos en amplias zonas de Estados Unidos. Por ejemplo, en 2002, la Oficina Federal de Investigaciones, FBI, descubrió información emanada del Medio Oriente de que hackers estaban estudiando las instalaciones de generación eléctrica, transmisión, almacenamiento de agua, distribución y gas de sistemas digitales SCDA utilizado para controlar los servicios del área de la Bahía de San Francisco en California.[14] Teóricamente, los hackers podrían inhabilitar el SCDA o aún tomar control del sistema a fin de inhabilitar las compuertas de represas o controlar cientos de miles de voltios de energía eléctrica.

Es ampliamente conocido que Al-Qaeda está especialmente inclinada a las instituciones financieras con el fin de robar fondos, interrumpir el curso normal de negocios, crear distracciones costosas y en general derivar pánico.[15] Un ataque cibernético coordinado significaría mucho más que el inconveniente de cerrar los cajeros automáticos. Incluiría la transferencia de millones de dólares de cuentas bancarias.

Aparte del ataque cibernético, las fuerzas de orden público también deben considerar el escenario donde el terrorista lleve a cabo un ataque real con explosivos convencionales contra un SCDA o su equivalente, tal vez en asocio con un ataque cibernético. Un ataque terrorista suicida dirigido a un edificio que contiene uno de los principales proveedores de servicios Internet sería devastador.

Otras posibilidades de ataque son igualmente posibles. En un artículo de 2004 en *Computerworld Magazine*, Peiter Zatka, un experto en seguridad, expresó inquietudes acerca de los diferentes tipos de amenazas cibernéticas.[16] Zatka alertó que la verdadera destrucción puede no ocurrir del ataque cibernético, sino de amenazas internas. Una amenaza interna existe cuando un hacker infiltra una red interna y luego, en vez de ocasionar un rechazo inmediato de un servicio u otro tipo de daño, permanece invisible al interior de

14 Ver Gellman, Barton. "Se temen ataques cibernéticos por Al-Qaeda," TechNews.com. Junio 27, 2002

15 Ver Beth Guard, Mary. "Amenazas Físicas y Digitales a la Instituciones Financieras en los Albores de Ataques Terroristas", Bankers Online, 2001

16 Ver Zatko, Pieter. "Al interior de la amenaza interior", Computerworld, Junio 10, 2002

"Las universidades y los proveedores del servicio de red son los principales objetivos destinados a recolectar cuentas y credenciales para acceder a las redes internas de corporaciones debido a que tienen conexiones a red de alta velocidad que transportan una cantidad sustancial de tráfico para múltiples propósitos"

la red a fin de espiar. Los infiltradores utilizan una técnica "sniffing" (oler), a fin de adquirir la información de cuentas requerida para tener acceso a la red. Esto le permite a los interceptadores la capacidad de obtener toda la información que pasa a lo largo de la línea de la red, incluyendo nombres de usuarios y códigos. Al permanecer en condición no detectada, el infiltrador con frecuencia altera la encriptación y las aplicaciones de comunicación para poder copiar los datos que entran y salen de las terminales de control hacia diversas secciones escondidas del sistema.

"Las universidades y los proveedores del servicio de red son los principales objetivos destinados a recolectar cuentas y credenciales para acceder a las redes internas de corporaciones debido a que tienen conexiones a red de alta velocidad que transportan una cantidad sustancial de tráfico para múltiples propósitos".[17]

III. Protección del mundo cibernético

A pesar del hecho de que los criminales cibernéticos le cuestan a los negocios y a los consumidores hasta $10 mil millones al año con virus y fraude de identidad, las compañías tecnológicas se han resistido a los llamados del gobierno a producir un mejor software y unas redes más fuertes.[18] De manera similar, los propietarios de la infraestructura pública crítica son igualmente renuentes a compartir la información necesaria acerca de sus operaciones con otras compañías o con el gobierno. En parte, se preocupan de que sus competidores obtengan acceso a datos exclusivos de la compañía compartidos con el gobierno bajo la Ley de Información Libre, Foia, u otras fuentes.[19] Entre más pronto las instituciones compartan información acerca de las vulnerabilidades de seguridad, más rápidamente podrán todas las organizaciones implementar contramedidas para protegerse contra los terroristas cibernéticos.

La Estrategia Nacional para Aseguramiento del Ciberespacio[20] y la Estrategia Nacional para la Protección Física de Infraestructuras Críticas y Activos Claves fueron emitidas a mediados de 2003. Estas dos estrategias están diseñadas para ayudarle a Estados Unidos a asegurar el mundo cibernético estableciendo tres objetivos principales: (1) prevenir ataques cibernéticos contra la infraestructura crítica de Estados Unidos, (2) reducir la vulnerabilidad nacional a los ataques cibernéticos, y (3) reducir los daños y el tiempo de recuperación de los ataques cibernéticos cuando estos ocurran.

IV. La Ley Patriota y lucha contra el ciberterrorismo

Sin duda, la más conocida legislación asociada con los ataques terroristas del 11 de septiembre de 2001 es "*La Ley para unir y fortalecer a Estados Unidos proporcionando herramientas apropiadas requeridas para interceptar y obstruir al terrorismo de 2001*", o sencillamente la *Ley Patriota*.[21] Diseñada como una herramienta para ayudar a las fuerzas de orden público a destruir células terroristas y sus bases de operaciones, la Ley Patriota fue aprobada por una abrumadora mayoría en el Congreso y fue firmada como Ley por el Presidente Bush el 26 de octubre de 2001.[22] La Ley Patriota contiene una variedad mixta de disposiciones

Entre más pronto las instituciones compartan información acerca de las vulnerabilidades de seguridad, más rápidamente podrán todas las organizaciones implementar contramedidas para protegerse contra los terroristas cibernéticos.

17 Id

18 Krim, Jonathan. "Se solicitan metas Estados Unidos para seguridad del software; fuerza de tarea sugiere regulación limitada". Washington Post, Abril 2, 2002, en E2.

19 Ver Verton, Dan. Hielo negro: la amenaza invisible del terrorismo. 249, (2003)

20 Ver página web de la Casa Blanca sobre Estrategia Nacional para Asegurar el Ciberespacio, http://www.whitehouse.gov/pcipb.

21 La Ley para unir y fortalecer a Estados Unidos proporcionando herramientas apropiadas requeridas para interceptar y obstruir al terrorismo de 2001, Pub. L. No. 107-56. 115 Stat. 272 (Octubre 26, 2001). La ley fue aprobada por el Senado por una inmensa mayoría del 98-1. 147 Cong. Rec. S11,059,60 (Octubre 25, 2001). La Cámara de Representantes aprobó su versión por una similar mayoría de 357-66. 147 Cong. Rec. H7224 (Octubre 25, 2001) Ver también, la página web del Centro de Información Privada Electrónica en la Ley Patriota EE.UU.

22 Ibíd.

penales encaminadas tanto a la investigación de presuntos terroristas como a eliminar las fuentes de financiación y apoyo de las organizaciones terroristas. No obstante, dado que la mayoría de las disposiciones en la Ley Patriota reforman o agregan texto a leyes federales existentes, con frecuencia es difícil medir el total impacto de muchas de las disposiciones a primera vista. Por ejemplo, la Sección 203 de esta ley, reforma las Normas Federales de Procedimiento Penal, FRPC[23] para permitir la información presentada ante el Gran Jurado con otras agencias interesadas si esta se relaciona con inteligencia externa; la Sección 219 de la Ley Patriota reforma FRPC[24] para autorizar órdenes de búsqueda en toda la nación en casos de terrorismo, y la Sección 213 de la Ley agrega un subparráfo a 18 U.S.C. Sección 3130ª a fin de autorizar notificación demorada de la ejecución de una orden de búsqueda sobre ciertas condiciones.

En breve, la utilización de dispositivos de interceptación bajo la Ley Patriota ahora permite interceptar todo tipo de actividad privada en Internet y le facilita a las fuerzas públicas recolectar información privada comunicada aún en correos electrónicos personales. Un dispositivo de interceptación de llamadas entrantes y salientes utilizado en asocio con Internet le permite a las agencias federales capturar todos los encabezamientos de los correos electrónicos que salen y entran a una cuenta de correo electrónico, lista de todos los servidores a que un sospechoso acceda, rastreo de cualquier persona que ingrese a una cierta página web y rastreo de todas las páginas web a que un sospechoso en particular pueda llegar a acceder.[25] Por consiguiente, con una nueva definición, las interceptaciones, captura y rastreo ahora le permiten a las agencias federales incluir no sólo las líneas telefónicas, sino también Internet, correo electrónico, navegación por la web y cualquier otra forma de comunicación electrónica.

Una de las disposiciones más controvertidas de la Ley Patriota es la sección 213, que otorga a las agencias federales la capacidad de llevar a cabo registros secretos cuando están armadas de la orden judicial de causa probable. La "Sección 213 de la Ley Patriota elimina el requisito previo de que las fuerzas de orden público suministraran a una persona objeto de una orden de registro notificación oportuna sobre el registro.[26] Conocidas como "sneak and peak" (registros

23 FRCP 6(e)(3)(C)

24 FRCP 41(a)

25 Ibíd.

26 Ibíd

secretos), estas búsquedas le permiten a las fuerzas de orden público la autoridad de registrar y confiscar cualquier objeto o registro tangible sin notificación a su propietario o poseedor cuando la Corte encuentre "*necesidad razonable*" para la acción. Aun cuando no se establece un límite de tiempo para la notificación al sujeto, la ley común sugiere que es cuestión de días y no de semanas.

No obstante la retórica, los registros secretos no pueden llevarse a cabo sin una orden judicial emitida por un juez neutral y distanciado. Además, a fin de llevar a cabo este tipo de registros, la Corte debe encontrar "*causas razonables para pensar que una notificación inmediata de la ejecución de la orden podría resultar en un efecto adverso*" en la investigación.[27]

Obviamente, la disposición sobre los registros secretos es una herramienta extremadamente valiosa puesto que les permite a las autoridades recoger evidencia sin "alerta inicial". Con frecuencia muchos terroristas o grupos de terroristas en "células durmientes", mantienen sólo domicilios temporales y se sabe que cambian de lugar muy rápidamente.

Curiosamente, hay muchos que se oponen a la *Ley Patriota* como una violación a las libertades civiles.

27 Ibíd

"A pesar de los esfuerzos por "diabolizar" la *Ley Patriota*, las disposiciones son de hecho un esfuerzo juicioso por detener futuros ataques terroristas, particularmente, en el reino del ciberterrorismo... la *Ley Patriota* es una de las herramientas más importantes que el Congreso le ha dado al gobierno para combatir el terrorismo y prevenir ataques terroristas de hecho, muchas de las disposiciones en la *Ley Patriota* se refieren a asuntos de debido proceso.

Según Gregory Nojeim, el director asociado de la oficina en Washington de Aclu: "*estas nuevas facultades sin límite podrían ser utilizadas contra los ciudadanos americanos que no están bajo investigación penal, inmigrantes que están dentro de nuestras fronteras legalmente, y también aquellos cuyas actividades de defensa de la Primera Enmienda podrían juzgarse como amenazas a la seguridad nacional por el Procurador General*".[28]

A pesar de los esfuerzos por "diabolizar" la *Ley Patriota*, las disposiciones son de hecho un esfuerzo juicioso por detener futuros ataques terroristas, particularmente, en el reino del ciberterrorismo. Comentando con los diversos gobiernos locales que aprobaron leyes contra la *Ley Patriota*, un vocero del Departamento de Justicia señaló que muchas de estas ordenanzas se basaban en información errónea acerca de la ley, y que la *Ley Patriota* es una de las herramientas más importantes que el Congreso le ha dado al gobierno para combatir el terrorismo y prevenir ataques terroristas[29] de hecho, muchas de las disposiciones en la Ley Patriota se refieren a asuntos de debido proceso.

V. Conclusión

Los avances americanos en ciber tecnología son insuperables, no obstante, como es frecuente, la fortaleza mayor de un país puede ser al mismo tiempo una debilidad crítica. La dependencia de Estados Unidos en el mundo cibernético abre nuevas vulnerabilidades a una clase diferente de ataque terrorista. Un ataque cibernético puede atacar un sistema de red de computadoras que puede dañar una infraestructura crítica. El ex-director del FBI, Louis Freesch, afirmó que "*el FBI piensa que el ciberterrorismo, el uso de la ciberherramienta para paralizar, degradar o negar infraestructuras críticas nacionales como la energía, transporte, comunicaciones, o servicios estatales, con el fin de forzar o intimidar a un gobierno o población civil, claramente es una amenaza emergente*".[30] Es una amenaza que debe ser confrontada con el mismo reconocimiento y seriedad de un ataque terrorista físico. A fin de asegurar a la nación contra el ciberterrorismo, los funcionarios de seguridad no deben llevar a pensar que las organizaciones terroristas como Al-Qaeda, carecen de los equipos y de los conocimientos necesarios para lanzar dicho ataque. Miembros altos de Al Qaeda ya han expresado su intención de atacar la economía y las infraestructuras de Estados Unidos utilizando Internet.

Estados Unidos debe poner atención a estas advertencias, una herramienta valiosa en este esfuerzo es la Ley Patriota junto con el marco general establecido por la Estrategia Nacional para asegurar el Ciberespacio. Desafortunadamente, el hábito complaciente de enfrentarse a amenazas conocidas no ha impartido el sentido de urgencia que, en última instancia, será necesario para proteger al mundo cibernético. Las disposiciones arriba mencionadas deben ser fortalecidas en años venideros de modo que el mundo cibernético sea un lugar tan seguro para la existencia como el mundo físico.

28 Ver Olson, Stefany. "Ley Patriota causa Inquietudes sobre la Intimidad" Cinetnews.com, 26 de octubre de 2001.

29 Ibíd

30 Ver Burton, Dan. Hielo negro: la amenaza invisible del terrorismo. 249 (2003)

CURRICULUM

Jeffrey F. Addicott. Profesor Asociado de Derecho y Director del Centro de Derecho Terrorista, St Mary´s University, Facultad de Derecho. Título (con honores) de la Universidad de Maryland; J.D., Universidad de Alabama, Facultad de Derecho; LL.M. Escuela de Derecho para Abogados Militares (JAG) LL:M: y S.J.D; Facultad de Derecho Universidad de Virginia.