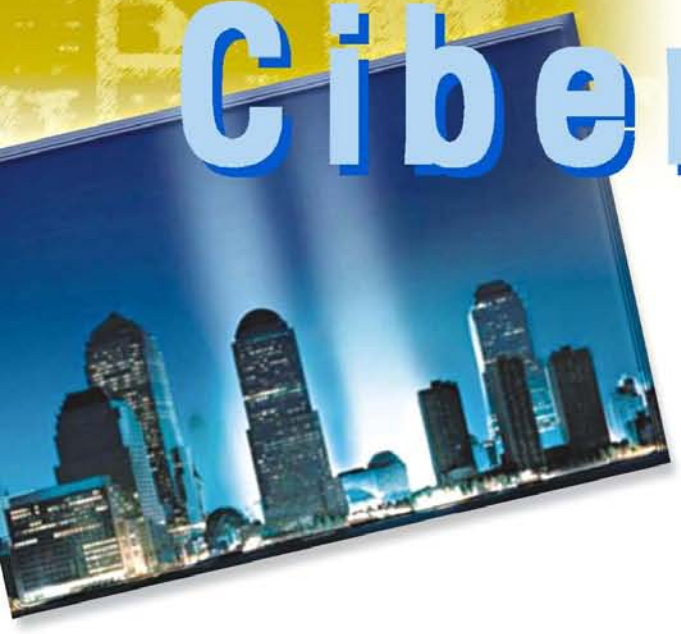
# Seguridad DE LA INFRAESTRUCTURA Y TERRORISMO Cibernético



## I. INTRODUCCIÓN

Mientras muchos registran la guerra contra el terrorismo a partir del 11 de septiembre de 2001, ahora es claro para todos que los Estados Unidos han sido blanco primario de los ataques terroristas perpretados por grupos radicales islámicos por muchos años. Desafortunadamente, desde una perspectiva retrospectiva, es aparentemente igual ya que los Estados Unidos no estaban preparados adecuadamente para defender su territorio en los innovadores ataques terroristas del 11 de septiembre de 2001.

PROFESOR AUXILIAR DE LEYES Y DIRECTOR, CENTRO DE LEY PARA EL TERRORISMO, UNIVERSIDAD DE LEYES ST. MARY. LICENCIADO (CON HONORES), UNIVERSIDAD DE MARYLAND; GRADO PROFESIONAL., UNIVERSIDAD DE LEYES DE ALABAMA., JUEZ GENERAL INTERCESOR DEL COLEGIO DE LEYES DE LA UNIVERSIDAD DE VIRGINIA.
ESTE DOCUMENTO FUE PREPARADO BAJO EL AUSPICIO DEL CENTRO DE LEY PARA EL TERRORISMO UBICADO EN LA UNIVERSIDAD DE LEYES ST. MARY., SAN ANTONIO TEXAS. EL OBJETIVO DEL CENTRO ES EXAMINAR AMBOS TEMAS POTENCIALMENTE LEGALES Y ACTUALES EN CUANTO A TERRORISMO. EL AUTOR DESEA AGRADECER A JORDAN LINSCOMB POR LA EXCELENTE AYUDA EN LA INVESTIGACIÓN.

The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) noted in their 360 page June 2004 report that the American intelligence and law enforcement agencies suffered from a "lack of imagination."[1] The government simply did not take seriously the possibility of terrorists using commercial airlines as precision weapons to attack buildings. The failure to appreciate the sophistication of the Al-Qa'eda terrorist network[2] opened the door for devastating attacks. Consequently, the United States was caught completely by surprise resulting in the loss of over 3,000 lives and billions of dollars in property loss.[3]

Since attacks of September 11, 2001, the government has crafted a variety of robust antiterrorism responses designed to disrupt terrorist networks and lessen the probability of future terrorist attacks from occurring.[4] Including the passage of the USA Patriot Act;[5] the creation of the Cabinet level post of Homeland Security;[6] and the establishment of United States Northern Command, in Colorado;[7] the United States has also engaged in other actions such as the preemptive use of military force against both rogue States, to include State supporters or sponsors of Al-Qa´eda styled terrorism; and the indefinite detention of suspected illegal alien terrorists and enemy combatants.

Without question, shifting the tactical focus from punishing those individuals, organizations, or nations who commit terrorist crimes or engage in aggression[8] to new broad methodologies designed to thwart such criminal acts in the first place has caused as sea change in how the government approaches terrorism prevention.

...shifting the tactical focus from punishing those individuals, organizations, or nations who commit terrorist crimes or engage in aggression to new broad methodologies designed to thwart such criminal acts...

[1] The National Commission on Terrorist Attacks Upon the United States closed on august 21, 2004.

[2] The Al-Qa'eda terror organization was founded in 1989 by a Saudi named Osama bin Laden. Dedicated to the destruction of the West the organization has demonstrated over the past three years that it is truly international in scope with the resources and personnel to coordinate sophisticated terror attacks on a scale never before seen. It is linked to a variety of terrorist groups from the Philippines to Indonesia and has trained tens of thousands of Arab and non-Arab militants in Afghanistan under the Taliban regime. Fueled by a super-fundamentalist Islamic radicalism its foot soldiers of hate gladly embrace death in their continuing quest for mass murder. *See* Michael Elliott, *Why the War on Terror Will Never End*, Time, may 26, 2003, at 29.

[3] Erika Goode, *A Day of Terror: The Psychology*, N.Y. Times, Sept. 12, 2001, at A13 [hereinafter Day of Terror]. On September 11, 2001, a total of 19 members of the terrorist al-Qa'eda network hijacked four domestic U.S. passenger aircraft while in flight (five terrorists in three of the planes and four in the fourth). The terrorists crashed two of the aircraft into the twin towers of the World Trade Center in New York. Another plane was crashed by the terrorists into the Pentagon, Washington, D.C., but the fourth plane was forced down by passengers into a field in Pennsylvania. According to a N.Y. Times tally, along with billions of dollars in property loss, approximately 3,067 were killed, not including the 19 terrorists. This figure includes 184 dead at the Pentagon (counting the 59 passengers on the hijacked plane) and 40 dead in Pennsylvania. *See Dead and Missing*, N.Y. Times, feb. 10, 2002, at A12, col. 1.

[4] *See The National Security Strategy of the United States of America*, The White House, Washington, D.C., Sept. 17, 2002, p. 15 [hereinafter *National Security Strategy*] (the so-called Bush Doctrine adopts the use of preemptive force in self-defense and is designed to prevent the marriage of Al-Qa'eda-styled terrorism with weapons of mass destruction).

[5] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (oct. 26, 2001). The bill passed the Senate by a landslide vote of 98-1. 147 Cong. Rec. S11,059-60 (daily ed. oct. 25, 2001). The House of Representatives passed their version by a similar lopsided vote of 357-66. 147 Cong. Rec. H7224 (daily ed. oct, 25, 2001).

[6] *See* Homeland Security Act of 2002, Pub L. No. 107-296, 116 Stat. 2135 (Nov. 5, 2002) [hereinafter Homeland Security Act]; *See generally* Editorial, *Seeking Homeland Security*, New York Post, June 7, 2002, at 32 (the department of Homeland Security incorporates more than 100 different government divisions from eight separate Cabinet departments into a single agency whose sole mission is homeland security).

[7] The U.S. Northern Command is located at Peterson Air Force Base in Colorado Springs, Colorado. It was established October 1, 2002 and is the single military headquarters focused on national defense and assisting the nation following a major natural disaster or man-made attack. There are currently about 500 military and civilian personnel assigned to the new command. *See* Vince Crawley, *9-11Means 24-7 Northern Command Scrutinizes all Threats – Man-Made or Natural*, Army Times, Jan. 19, 2004, at 18.

[8] Definition of Aggression, G.A. Res. 3314, 29 U.N. GAOR. Supp. No. 31, U.N. Doc. A/9631 (1957), at 142. The U.N. Definition of Aggression states in main part:

Article 1

Aggression is the use of armed force by a State against the sovereignty, territorial integrity, or political independence of another State, or in any manner inconsistent with the Charter of the United Nations ...

Article 2

The first use of armed force by a State in contravention of the Charter shall constitute *prima facie* evidence of an act of aggression...

Article 3

Any of the following acts, regardless of a declaration of war, shall ... qualify as an act of aggression:

(a) The invasion or attack by the armed forces of a State ... of another State or part thereof;

(b) Bombardment by the armed forces of a State against the territory of another State ...,

(c) The blockade of the ports or coasts of a State by the armed forces of another State;

(d) An attack by the armed forces of a State on the land, sea, or air forces, or marine and air fleets of another State;

(e) The use of armed forces of one State ... in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a State in allowing it territory, which it has placed at the disposal of another State to be used by that other State for perpetrating an act of aggression against a third State; or

(g) The sending by or on behalf of a State of armed bands, groups, irregulars, or mercenaries which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

La Comisión Nacional sobre los Ataques Terroristas en los Estados Unidos (Comisión 9/11) en su renombrado artículo de 360 páginas de junio de 2004 reportó que la inteligencia de los Estados Unidos y las Agencias de ejecución de leyes sufrieron una "falta de imaginación"[1]. El gobierno simplemente no tomó seriamente la posibilidad de que los ataques terroristas usaran aerolíneas comerciales con armas de precisión para atacar edificios. La falla en apreciar la sofisticación de la red terrorista Al-Qaeda[2] abrió las puertas a ataques devastadores. En consecuencia, los Estados Unidos fueron atrapados completamente por el factor sorpresa con el resultado de la pérdida de más de 3.000 vidas y billones de dólares en la pérdida de propiedades[3].

Desde los ataques del 11 de septiembre, el gobierno ha elaborado una variedad de respuestas antiterroristas diseñadas para dividir las redes terroristas y minimizar la probabilidad de futuros ataques terroristas[4]. Incluyendo el paso del acto patriótico de los Estados Unidos[5]; la creación de la Cabinas de Seguridad Territorial[6]; y el establecimiento del Comando Septentrional de los Estados Unidos, en Colorado[7]. Los Estados Unidos también han comenzado otras acciones tales como el uso preventivo de las Fuerzas Militares contra Estados que patrocinan o apoyan el estilo del terrorismo de Al-Qaeda y la detención indefinida de extranjeros ilegales que puedan ser terroristas sospechosos o terroristas combatientes.

Sin duda, el cambio del enfoque táctico desde castigar aquellos individuos, organizaciones o naciones que cometan crímenes terroristas o se inicien en la agresión[8] , hasta utilizar nuevos y amplios métodos para frustrar tales actos criminales, causando un cambio en cómo el gobierno dirige la prevención contra el terrorismo.

[1] La Comisión Nacional de Ataques Terroristas cerró el 21 de agosto de 2004.

[2] La organización terrorista Al-Qaeda fue fundada en 1989 por un árabe llamado Osama Bin Laden. Dedicada a la destrucción de Oriente. La organización ha demostrado en los últimos 3 años que realmente tiene alcance internacional con los recursos y el personal para coordinar sofisticados ataques terroristas, en una escala nunca vista. Está ligada a otras agrupaciones terroristas, desde Filipinas hasta Indonesia y ha entrenado miles de militantes árabes y no árabes en Afganistán bajo el régimen Talibán. Cargado por un super-fundamentalismo islámico radical, sus soldados de tierra, llenos de odio, felizmente abrazan la muerte con su continua ejecución, asesinatos masivos. Ver Michael Elliot. Porqué la Guerra sobre el terrorismo nunca finalizará. Times. 26 de mayo de 2003. (29)

[3] Goode Erika. Un día de terror: El psicólogo. NY. Times. (A. 13) 12 de septiembre de 2001. Sep. 11/01. un total de 19 miembros de la red terrorista Al-Qaeda secuestró cuatro aviones comerciales estadounidenses en vuelo (5 terroristas en 3 aviones y 4 en el cuarto). Los terroristas estrellaron dos de los aviones en las Torres Gemelas del World Trade Center en New York. Otro avión fue estrellado por los terroristas en el Pentágono, Washington D.C. pero el cuarto avión fue forzado aterrizar por los pasajeros en un campo de Pennsylvania. De acuerdo a un sondeo del NY. Times, billones de dólares en pérdidas de propiedades y aproximadamente 3.67 muertos, sin incluir los 19 terroristas. Esta figura incluye 184 muertes en el Pentágono (contando los 59 pasajeros del avión secuestrado) y cuarenta muertos en Pennsylvania. Ver Dead and Missing. New York Times, 10 de febrero de 2002 (A.12 col 1).

[4] Ver, the National Security Strategy of the United Status of America. La Casa Blanca. Washington D.C. 17 de septiembre de 2002 p.15. (La llamada doctrina Bush adopta el uso de fuerzas preventivas en auto-defensa y esta diseñada para prevenir los ataques terroristas de Al-Qaeda con armas de destrucción masiva)

[5] Unificando y fortaleciendo América proveyendo herramientas adecuadas, requeridas para interceptar obstruir acciones terroristas de 2001. Pub. L.No. 107-56-115 Stat.272 (26 de octubre de 2001 La ley fue presentada al Senado y ganó por gran mayoría: 98-1. 147Cong. Rec. S11. 059-60 (daily ed. Oct 25/01) La Cámara de Representantes pasó su versión por una votación similar 357-66. 147 Cong. Rec. H7224 (daily Oct 25/01)

[6] Ver. Homeland Security Act. 2002. Pub. L. No. 107-296. 116 Stat. 2135 (nov 5/02). ver la edición general, Seeking Homeland Security. New York Post. 7 de junio de 2002 art. 32 (el departamento de seguridad territorial incorpora más de 100 diferentes divisiones en el gobierno de ocho cabinas separadas, departamentos y las convierte en una sola agencia, la cual tiene como misión la seguridad territorial).

[7] El Comando Septentrional está localizado en la base aérea de la Fuerza Aérea, en Colorado, Springs. Fue establecida el primero de octubre de 2002 y es un solo cuartel militar enfocado a la defensa nacional y en asistir a la nación después de un desastre natural o un ataque planeado por humanos. Actualmente hay unos 500 militares y civiles como personal asignado al nuevo comando. Ver Vince Crawly. 9/11 Means24-7 Northern Command scrutinizes all Treats- man made or natural. Army Times. En 19.04 Art. 18.

[8] Definición y Agresión: G.A. Res. 3314329 U.N GAOR, Supp No. 31, U.N Doc A/9631 (1957). Art. 142. La definición de las Naciones Unidas de agresión:

Art. 1: la agresión es usada por las fuerzas armadas del Estado contra la soberanía, integridad territorial o la independencia política de otro Estado, o en algún otro asunto inconsistente con el estatuto de las Naciones Unidas...

Art. 2: el primer uso de la fuerza armada por el Estado en infracción del estatuto debe constituir prima facie como evidencia de un acto de agresión...

Art. 3: Algunos de los siguientes actos, Indiferente de la declaración de guerra, debe calificar como actos de agresión:

(a) La invasión o el ataque de fuerzas armadas de un estado... o de otro Estado o parte de eso:

(b) Bombardeo por fuerzas armadas de un Estado contra el territorio de otro Estado.

(c) El bloqueo de puertos o costas de un Estado, por fuerzas armadas de otro Estado.

en la tierra, en el mar, o en las fuerzas aéreas, o marinas, o flota aérea de otro Estado.

(d) Un ataque de las fuerzas armadas de un Estado, en la tierra, en el mar, o en las fuerzas aéreas, o marinas, o flora aérea de otro Estado.

(e) El uso de fuerzas armadas de un Estado... en infracción de las condiciones proveídas por un acuerdo a alguna extensión de su presencia en dicho territorio, más allá de la terminación del acuerdo.

(f) La acción del Estado permitiéndole al territorio, el cual ha sido colocado a disposición de otro Estado, para ser usado, por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado: o

(g) El envío de bandas armadas por parte de otro Estado, grupos irregulares o mercenarios quienes llevan actos con fuerzas armadas contra otro Estado, de tal gravedad, hasta sumar actos listados anteriormente o su involucramiento substancial en alguno de ellos.

...el cambio del enfoque táctico desde el castigar aquellos individuos, organizaciones o naciones quienes cometan crímenes terroristas o se inicien en la agresión, hasta utilizar nuevos y amplios métodos diseñados para frustrar tales actos criminales ...

Nevertheless, a new and deadly terrorist threat called cyber terrorism[9] is now emerging that may, as many commentators predict, catch the United States totally off guard. The same failure of recognition and lack of awareness prior to the terrorist air attacks of September 11, 2001 might be mimicking itself in the cyber world, and it could prove to be more crippling and deadly than anything imaginable. It is simply naïve to believe that terrorists will not adapt their weapons to attack cyber space.

The purpose of this article is to discuss the threat of cyber terrorism and to address some of the new tools that the United States is employing to address the threat. As stated, there is a growing body of evidence that a cyber terrorist attack will occur in the United States in the near future.[10] When one considers that terrorist organizations such as Al-Qa'eda and Hamas have been using computers, email, and encryption to support and finance their organizations for years, it is only logical to conclude that they are fully aware that cyber terrorism offers a low cost method of inflicting major damage and it is very difficult to trace.

**The purpose of this article is to discuss the threat of cyber terrorism and to address some of the new tools that the United States is employing to address the threat.**

## II. THE THREAT OF CYBER TERRORISM

The modern world we have created is totally dependent on the workings of the Internet, computer databases and software of the cyber world. Without question, the cyber realm is fully incorporated into our everyday lives and touches almost everything we do or think. Apart from serving as a fantastic communication medium, the cyber world regulates all aspects of our infrastructure to include water, electricity, banking, transportation, technology, agriculture, medical, nuclear facilities, waste management, government services, etc. This fact has not only spawned the era of cyber crime, it has also given rise to the specter of cyber terrorism.

Cyber terrorism is the employment of various computing resources to intimidate or coerce another (usually the government) in furtherance of specific objectives. One commentator has defined cyber terrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non combatant targets by sub national groups or clandestine agents."[11] Accordingly, cyber terrorism involves activities to disrupt, corrupt, deny, or destroy information contained in computers or computer networks. Of course, not all acts of cyber crime would meet the definition of cyber terrorism.

In the lexicon of computer terminology there are three types of cyber criminals: (1) script-kiddies, (2) hackers, and (3) crackers. Cyber terrorists belong to the most serious cyber criminal, the cracker.[12] Script-kiddies are low level computer criminals. They usually download various computer packages and tools from the Internet and use them to exploit security weaknesses in order to, for example, deface a website or harasses certain users. The hacker is more sophisticated than the script-kiddie and uses his increased computer skills to penetrate secure systems, generally for the thrill of the accomplishment. The more secure the system penetrated, the greater the thrill. In fact, in august 2004, the public learned that hackers had penetrated hundreds of "powerful computers at the Defense Department and U.S. Senate" and used them to send spam e-mail.[13] On the other hand, the cracker is the most insidious cyber criminal. The cracker attacks computer systems for true criminal purposes to include blackmail, espionage, or for pure maliciousness, like virus writers. "Cyberterrorists are grouped with crackers because they share similarly malevolent purposes..."[14]

---

[9] The term cyber terrorism was coined by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California.

[10] *See* Mary Beth Guard., "Physical and Digital Threats to Financial Institutions in the Wake of the Terrorist Attacks," *Bankers Online*, 2001.

[11] *See* Mark Pollit, "Cyberterrorism: Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference*, october 1997, at 285-289.

[12] *See* Reid Skibell, "CyberCrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act," 18 *Berkeley Tech. LJ* 909, Summer 2003.

[13] Jon Swartz,"Hackers Jijack Federal Computers, USA Today, aug.31, 2004, at 1B.

[14] Id. at 921

Sin embargo, un nuevo terrorismo llamado terrorismo cibernético[9], está emergiendo. Como muchos analistas predicen, pueden atrapar a los Estados Unidos con la guardia abajo. La misma falta de reconocimiento y la falta de conciencia previa a los ataques aéreos terroristas del 11 de septiembre de 2001 pueden estar imitándose en el mundo cibernético, y pueden demostrar ser más mortales que cualquier cosa que se pueda imaginar. Es simplemente ingenuo creer que el terrorismo no adapte sus armas para atacar el ciber-espacio.

El propósito de este artículo es discutir la amenaza el terrorismo cibernético y mencionar algunas de las nuevas herramientas que los Estados Unidos están empleando para combatir la amenaza. Como fue mencionado, hay una creciente evidencia de ataques de terrorismo cibernético en los Estados Unidos en un futuro cercano[10]. Cuando se considera que organizaciones terroristas tales como Al-Qaeda y Hamas han estado utilizando computadores, correos electrónicos para apoyar y financiar sus organizaciones por años, es lógico, concluir que ellos están completamente concientes que el terrorismo cibernético ofrece un método de bajo costo para imponer un daño de grandes proporciones el cual es muy difícil de rastrear.

## II. LA AMENAZA DEL TERRORISMO CIBERNÉTICO

El mundo moderno que hemos creado es totalmente dependiente de los trabajos de Internet, bases de datos y programas del mundo cibernético. Sin lugar a dudas, el mundo cibernético está completamente incorporado en nuestra vida diaria y toca casi todo lo que hacemos o pensamos. A parte de servir como un medio de comunicación fantástico, el mundo cibernético regula todos los aspectos de nuestra infraestructura incluyendo el agua, la electricidad, los bancos, el trasporte, la tecnología, la agricultura, la medicina, recursos nucleares, el manejo de desperdicios, servicios gubernamentales, etc. Este hecho no sólo ha engendrado la era del crimen cibernético, sino que también ha levantado el espectro del terrorismo cibernético.

El terrorismo cibernético se define como el empleo de varios recursos computarizados para intimidar u obligar a otros (generalmente el gobierno) a cumplir objetivos específicos. Un analista ha definido el terrorismo cibernético como "ataque político premeditado contra la información, sistemas computarizados, programas de computadores, y bases de datos" lo cual resulta en violencia contra blancos no combatientes de grupos subnacionales o agentes clandestinos[11]. En consecuencia, el terrorismo cibernético involucra actividades para dividir, corromper, negar, o destruir información contenida en computadores o redes de computadores. Por supuesto, no todos los actos de crimen cibernético adoptan la definición de terrorismo cibernético.

En el léxico cibernético hay tres clases de criminales: (1) script-kiddies (bromistas), (2) hackers (computo maniaco), y (3) crackers (petardos). Los terroristas cibernéticos The crackers pertenecen al más serio crimen cibernético[12]. Los Script-kiddies pertenecen a un bajo nivel de crimen cibernético: Ellos generalmente bajan varios paquetes de computador y herramientas de Internet y las utilizan para explotar las debilidades de seguridad de la red. Por ejemplo, para borrar sitios en la Web o acosar algunos usuarios. Los hackers son más sofisticados que los script-kiddies y usan sus destrezas para penetrar en los sistemas de seguridad, generalmente solo por la emoción de lograrlo. De hecho en agosto de 2004, el público aprendió que los hackers han penetrados cientos de computadores poderosos en el Departamento de Defensa y el Senado de los Estados Unidos y los han usado para enviar correos spam[13]. Por otra parte, el cracker, es el más insidioso criminal cibernético. El cracker ataca los sistemas de los computadores por verdaderos motivos criminales incluyendo chantaje, espionaje o por pura maldad, como los creadores de virus. "los terroristas cibernéticos están agrupados con los crackers" porque ellos comparten propósitos maléficos similares"[14].

[9] El término terrorismo cibernético fue acuñado por Barry Collin, un investigador del Instituto para la Seguridad y la Inteligencia en California.
[10] Ver Mary Beth Guard., "Physical and digital Tretas to financial Institutions in the Wake of Terrorist Attacks". Bankers Online. 2001
[11] See Mark Pollit, "Cyberterrorism: Fact or Fancy.? Proceedings of the 20th National Information Systems Security Conference, oct 1997, at 285-289
[12] Ver Reid Skibell,"CyberCrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act" 18 Berkeley Tech. LJ 909, Summer 2003.
[13] Jon Swartz,"Hackers Jijack Federal Computers, USA Today, aug.31, 2004, at 1B.
[14] Id. at 921

**El propósito de este artículo es discutir la amenaza del terrorismo-cibernético y dirigir algunas de las nuevas herramientas que los Estados Unidos están empleando para combatir la amenaza.**

Those unfamiliar with the term cyber terrorism view the concept to mean an attack on the Internet. This is far too simplistic a view. A cyber attack could be used to destroy not only the electronic, but also the physical infrastructure of a country. This is true because some of the nation's most important infrastructures such as defense systems, chemical and hazardous materials, water supply systems, transportation, energy, finance systems, and emergency services are controlled by centralized computer networks called Supervisory Control and Data Acquisition (SCDA) systems. SCDA systems provide the "brain power" to manage critical infrastructures. A successful cyber terror attack on even a single SCDA could cause massive economic and physical damage throughout large portions of the United States.

For example, in 2002, the Federal Bureau of Investigation (FBI) uncovered information emanating out of the Middle East that hackers were studying the electrical generation, transmission, water storage, distribution and gas facilities of SCDA digital systems used to control the utilities of the San Francisco Bay Area in California.[15] Theoretically, hackers could disrupt the SCDA or even take command of the system in order to disable the flood gates or control hundreds of thousands of volts of electric energy. In fact, this type of activity has already occurred in Australia.

In 2002 a hacker was arrested in Australia for breaking into the SCDA of an Australian sewage and water treatment plant and pumping one million liters of sewage into the environment. This was the first reported instance of a hacker successfully breaking into a system and causing massive damage.[16] It is a harbinger of things to come.

Indeed, the activity of all kinds of cyber crime is on the increase. A study released in june 2004 found that cyber attacks on financial institutions have more than doubled from the previous year.[17] Studies regularly demonstrate that the majority of Internet professionals believe a major attack on Wall Street or other banking institutions is imminent.[18] It is well known that Al-Qa'eda is especially attracted to financial institutions in order to steal funds, disrupt normal business, create costly distractions and to generally cause panic.[19]

[15] *See* Barton Gellman, "Cyber Attacks by Al-Qa'eda Feared," *TechNews.com*, June 27, 2002.
[16] Ronald N. Weikers & Kevin P. Cronin, "Electronic Security Risks and the Need for Privacy," Data. Sec. & Privacy Law: Combating Cyberthreats, Spring 2004.
[17] Linda Rosencrance, "Survey: Cyberattacks on the Rise at Financial Institutions," *Computerworld*, June 2, 2004.
[18] *See* Brett Stohs, "Cyber Crime," 2002 *Duke L. & Tech. Rev* 18, sept. 2002.
[19] *See* Mary Beth Guard, "Physical and Digital Threats to Financial Institutions in the Wake of the Terrorist Attacks," *Bankers Online*, 2001.

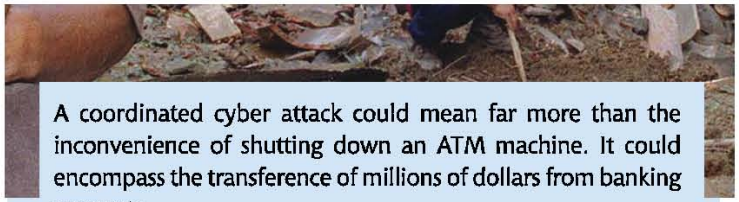
Para aquellos que no están familiarizados con el término de terrorismo cibernético, examinaremos el concepto para saber lo que significa un ataque en Internet. Estamos lejos de un examen simplista. Un ataque cibernético podría ser utilizado para destruir no sólo lo electrónico, sino también, la infraestructura física de un país. Esto es verdad, porque las redes de computadores centralizan el Control de Supervisión y Adquisición de base de datos de sistemas de control de químicos y materiales peligrosos; sistemas de abastecimiento de agua, trasporte, energía; sistemas de financiamiento y servicios de emergencia. El Sistema de Control de Supervisión y Adquisición de las base de datos (SCSAD) provee el "poder cerebral" para manejar infraestructuras críticas. Un ataque terrorista cibernético en un solo SCSAD podría causar un daño masivo económico y físico a lo largo de los Estados Unidos.

Por ejemplo, en el 2002, la Agencia Federal de Investigación (FBI) descubrió información que emanaba del Medio Oriente, en donde hackers estaban estudiando la generación de electricidad, de transmisión, el represamiento del agua, medios de gas y su distribución a través de sistemas digitales del SCSAD usado para controlar empresas de servicios públicos de San Francisco y del área de California[15]. Teóricamente, los hackers podrían interferir el SCSAD hasta tomar el control del sistema para deshabilitar las compuertas o controlar cientos de miles de voltios de electricidad. De hecho, esta clase de actividad ha sucedido en Australia.

En el 2002 un hacker fue arrestado en Australia por haber interrumpido en el SCSAD del alcantarillado y la planta de tratamiento de agua australiano y bombear un millón de litros de agua contaminada en el medio ambiente. Este fue el primer reporte que un hacker haya triunfado irrumpiendo en el sistema y causado un daño masivo[16].

Verdaderamente, la actividad de toda clase de crímenes cibernéticos se está incrementando. Un estudio revelado en junio de 2004 encontró que los ataques cibernéticos a instituciones financieras se han duplicado con respecto a años anteriores[17]. Los estudios regularmente muestran que la mayoría de los profesionales en Internet creen que un gran ataque al Wall Street o a otra institución bancaria es inminente[18]. Es bien conocido, que Al-Qaeda está especialmente atraído hacia las instituciones financieras para robar fondos, desgajar negocios normales, y crear distracciones costosas además de causar pánico en general[19].

[15] Ver Barton Gellman, "Cyber Attacks by Al-Qaeda Feared", Tech News.com, jun 27/02
[16] Ronald N.Weikers & Kevin P. Cronin, " Electronic Security risks and the Need forPrivacy" Data. Sec.&Privacy Law: combating Cyberthreats. Spring 2004
[17] Linda Rosencrance, "Survey: Cyberattacks on the Rise at Financial Institutions", Computerworld, jun 2 /04
[18] Ver Brett Stohs, :cyber Crime,: 2002 Duke L. & Tech, Rev 18, sep. 2002
[19] Ver Mary Beth Guard, "Physical and digital Tretas to financial Institutions in the Wake of Terrorist Attacks", Bankers Online, 2001



A coordinated cyber attack could mean far more than the inconvenience of shutting down an ATM machine. It could encompass the transference of millions of dollars from banking accounts.

Apart from a cyber attack, law enforcement must also consider the scenario where terrorists conduct an actual conventional explosives attack on a SCDA or its equivalent, perhaps in conjunction with a cyber attack. A terrorist suicide attack aimed at a building that contains a major Internet service provider would be devastating.

Other possibilities for attack are equally possible. In a 2004 article in *Computerworld Magazine*, Peiter Zatka, a security expert, expressed concerns about a different type of cyber threat.[20] Zatka warned that the real destruction might not occur from cyber attacks, but from insider threats. An insider threat exists when a hacker infiltrates an internal network and then, instead of causing an immediate denial of service or other type of harm, remains invisible inside the network in order to spy. The infiltrators use a technique called "sniffing" in order to acquire account information needed to access the network. This allows the interceptors the ability to obtain all the information that passes along the network line, including usernames and passwords. Remaining undetected, the insider often alters encryption and communication applications in order to copy input and output data from the control terminals to various hidden sections on the system. "Universities and network service providers are prime targets for harvesting of accounts and credentials to access the internal networks of corporations because they have high speed network connections that carry substantial amounts of traffic for a multitude of purposes."[21]

In testimony before the United States Senate in 2004, the Deputy Director of the FBI's cyberdivision stated: "The FBI predicts that terrorist groups will either develop or hire hackers, particularly for the purpose of complementing large scale attacks with cyberattacks."[22] There is no doubt that Al-Qa'eda styled terrorists are studying means to attack Western infrastructure by means of cyber space. If they are successful, the world could suffer an "electronic Pearl Harbor."

## III. PROTECTING THE CYBER WORLD

One thing is certain, as the sophistication of all forms of cyber crime increases, so does the threat to the cyber world.

[20] *See* Peiter Zatko, "Inside the Insider Threat," *Computerworld*, june 10, 2004.
[21] *Id.*
[22] *Cybercrime Law Report*, "On the Hill Hacking for Terror," march 8, 2004.

Un ataque cibernético coordinado podría significar mucho más que el inconveniente de un cajero automático cerrado. Esto podría abarcar la transferencia de millones de dólares en cuentas bancarias.

Aparte de un ataque cibernético, la ejecución de la ley debe también considerar el escenario donde los terroristas conduzcan un ataque explosivo en un SCAD o su equivalente, tal vez, en unión con un ataque cibernético. Un ataque terrorista suicida dirigido a un edificio que contiene un gran servicio proveedor de Internet sería devastador.

Otras posibilidades de ataque son igualmente posibles. En un artículo publicado en la Revista de Computer world en el 2004, Peiter Zatka, experto en seguridad expresó su preocupación sobre diferentes clases de amenazas cibernéticas[20]. Zaka advirtió que la destrucción real podría no ocurrir como ataques cibernéticos, sino de amenazas internas. Una amenaza interna existe cuando un hacker se infiltra en una red interna y después, en vez de causar una negación inmediata del servicio u otra clase de daño, permanece invisible dentro de la red para poder espiar. Los filtradores usan una técnica llamada "olfatear" para adquirir cuentas de información para tener acceso a la red. Esto le permite a los interceptores tener la habilidad para obtener toda la información que pasa a lo largo de la red, eso incluye, nombre de los usuarios y claves. Permaneciendo indetectable, el intruso, a menudo altera la encriptación y las aplicaciones de comunicación para copiar la información que entra y sale de las terminales de control de varias secciones ocultas en el sistema. "Las universidades y los proveedores de servicio en la red son los bancos primarios para cosechar cuentas y credenciales para acceder a las redes internas de las corporaciones, porque ellos tiene conexiones de red de alta velocidad que llevan sumas substanciales de tráfico para múltiples propósitos"[21].

En un testimonio anterior, en el Senado de los Estados Unidos en el 2004, el director y diputado de la ciber división del FBI declaró: "El FBI predice que grupos terroristas desarrollarán o contratarán hackers, particularmente, con propósitos de complementar grandes ataques a escala con ataques cibernéticos"[22]. No hay duda que Al-Qaeda con terroristas especializados están estudiando nuevos medios de ataque contra la infraestructura accidental por medios ciber espaciales. Si ellos lo logran, el mundo podría sufrir un "Pearl Harbor electrónico".

## III. PROTEGIENDO EL MUNDO CIBERNÉTICO

Una cosa es segura: mientras la sofisticación de todas las formas del crimen cibernético aumenta, también se aumenta la amenaza al mundo cibernético.

[20] Ver Peiter Zatko, "Inside the Insider Threat," Computerworld, jun10, 2004
[21] Ibid
[22] Cybercrime Law Report, " On the hill Hacking for Terror," marz 8, 2004

Considering that the super highway of the cyber world is composed of hundreds of thousand of interconnected computers, servers, switches, and fiber optics that allows our critical infrastructures to function, no single institution is safe. Furthermore, since 85-90% of America's critical infrastructure is privately owned[23] it is imperative that the government and industry join together in a unified manner to establish proactive and reactive strategies. In any plan, the need for timely and accurate information is essential.

Despite the fact that cyber criminals cause businesses and consumers as much as $10 billion a year through viruses and identity fraud, technology companies have largely resisted government calls to produce better software and stronger networks.[24] Similarly, the owners of the critical public infrastructure are equally reluctant to share necessary information about their operations with other companies or the government. In part, they are worried that their competitors will gain access to exclusive company data that is shared with the government through the Freedom of Information Act (FOIA) or other sources.[25]

**A study released in June 2004 found that cyber attacks on financial institutions have more than doubled from the previous year.**

Finding an effective way to encourage private industry to respond to the challenge of cyber terrorism has been problematic. The Clinton administration took the initial steps to address the vulnerabilities of the nation's infrastructure to cyber crime.

In a Presidential directive, several of the most critical infrastructures of the nation – both public and private - were identified to include telecommunications, energy, finance, and emergency services.

Although the Clinton directive called for a voluntary partnership between government and private industry, few private companies exhibited interest in joining the effort, citing loss of valuable information in a competitive market based economy. Two concerns were advanced. First, if a company revealed that a cyber terror event had breached their system that revelation could cause loss of confidence in the soundness of the business. Second, if a company revealed how its security system operated, competitors might use that information to gain a competitive advantage.

[23] Brett Stohs, "Cyber Crime," 2002 *Duke L. & Tech. Rev* 18, sept. 2002.
[24] Jonathan Krim, "U.S. Goals Solicited on Software Security; Task Force Suggests Limited Regulation," *Washington Post*, apr. 2, 2003 at E2.
[25] *See* Dan Verton, Black Ice: The Invisible Threat of Terrorism, 249, (2003).

Considerando que la superautopista del mundo cibernético está compuesta de cientos de miles de computadores interconectados[23], servidores, interruptores, y fibras ópticas que permiten funcionar nuestra infraestructura crítica... ni una sola institución está segura. Además, desde que el 85-90% de la infraestructura crítica americana es de la empresa privada es imperativo que el gobierno y las industrias se unifiquen para establecer estrategias reactivas y preactivas. En cualquier plan, la necesidad de la información precisa y a tiempo es esencial.

A pesar del hecho que los criminales cibernéticos le cuestan a las compañías y a los consumidores más de $ 10 billones de dólares al año debido a virus y fraudes de identidad, las compañías de tecnología han resistido fuertemente los llamados del gobierno para producir mejores programas y redes más fuertes[24]. Similarmente, los dueños de la infraestructura pública crítica están, igualmente, renuentes a compartir información necesaria acerca de sus operaciones con otras o el gobierno. En parte, ellos están preocupados que sus competidores obtengan acceso a datos exclusivos de la compañía que es compartida con el gobierno a través de la ley de Libre Información (LLI) u otras fuentes[25].

**Un estudio revelado en junio del 2004 encontró que los ataques cibernéticos a instituciones financieras se han duplicado con respecto a años anteriores.**

Encontrar un camino efectivo para animar a la industria privada a responder al reto del terrorismo cibernético ha sido problemático. La administración Clinton dio un paso inicial para dirigir las vulnerabilidades de la infraestructura de la nación contra el crimen cibernético.

En una directiva presidencial, varias de las infraestructuras más críticas de la nación; pública y privada fueron identificadas para incluir las telecomunicaciones, la energía, las finanzas y los servicios de emergencia.

A pesar que la directiva Clinton llamó a una asociación voluntaria entre el gobierno y la industria privada, pocas compañías mostraron interés en unir esfuerzos, mencionando pérdida de información de valor, basado en la economía de un mercado competitivo. Se avanzó en dos asuntos. Primero, si una compañía revelaba que un evento terrorista cibernético había violado sus sistemas y que la revelación pudiera causar pérdida de la entera confidencialidad del negocio. Segundo, si una compañía revelaba cómo sus sistemas de seguridad operaban, los competidores podrían utilizar esa información para obtener ventajas competitivas.

23. Brett Stosh, "Cyber Crime," 2002 Duke L. & Tech. Rev. 18, sep 2002
24. Jonathan Krim, "USA Goals Solicite don Software Security; Task Force Suggests Limited Regulation", Washington Post, apr.2 2003 at E2
25. Ver Dan Verton, Black Ice: The Invisible threat of Terrorism, 249, 2003.

On the other hand, without disclosure of information about hackers and the possible weak points of security systems, it is difficult for institutions to know what vulnerabilities exist within their security systems. The sooner that institutions share information about security vulnerabilities the quicker all organizations can implement counter measures to protect themselves from cyber terrorists.

Building on the Clinton approach, the Bush administration has taken a number of similar steps designed to develop public-private alliances to combat cyber terrorism. Like Clinton, the Bush administration saw the private sector as best equipped to tackle the potential threat of cyber terrorism. This premise is based on the fact that private sector technologies created cyber space and continues to evolve new avenues. Accordingly, number of new laws and policy directives have been passed to better secure the nation from a cyber attack.

The National Strategy to Secure Cyberspace[25] and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets were released in mid 2003. These two strategies are designed to help America secure the cyber world by establishing three main objectives: (1) prevent cyber attacks against America's critical infrastructure, (2) reduce national vulnerability to cyber attacks, and (3) reduce damage and recovery time from cyber attacks when they do occur.

The main priority of the National Strategy to Secure Cyberspace is the establishment of a national cyberspace security response system. The DHS is in the process of perfecting a response system that joins the government and the private sector together in order to provide for specific analysis, warning information and a crisis management response if a major cyber attack occurs. The plan also creates a national cyberspace security threat and vulnerability reduction program. This program would make an effort to identify and punish possible attackers, locate and remediate the existing vulnerabilities, and develop new systems and technology that would reduce future vulnerabilities.

[25] See the White House Web site on The National Strategy to Secure Cyberspace. http://www.whitehouse.gov/pcipb.

Por otra parte, si la divulgación de la información sobre los hackers y los posibles puntos débiles de los sistemas de seguridad, es difícil para las instituciones saber qué vulnerabilidades existen en sus sistemas de seguridad. Entre más pronto las instituciones compartan información sobre la vulnerabilidad en la seguridad, más rápido podrán las organizaciones implementar medidas para protegerse de los terroristas cibernéticos.

Construyendo sobre el acercamiento que hizo Clinton, la administración Bush ha tomado una gran cantidad de pasos diseñados para desarrollar alianzas público-privadas para combatir los terroristas cibernéticos. Así, igual que Clinton, la administración Bush vio el sector privado mejor equipado para atajar la potencial amenaza del terrorismo cibernético. Esta premisa, está basada en el hecho que la tecnología del sector privado creó el ciberespacio y continúa su evolución a nuevas avenidas. En consecuencia, un sin número de leyes y políticas directivas han sido creadas para mejorar la seguridad de la nación contra ataques cibernéticos.

La Estrategia Nacional para Asegurar el ciber-espacio[26] y la Estrategia Nacional para la Protección Física de Infraestructuras Críticas y Recursos Claves fueron lanzadas a mediados de 2003. Estas dos estrategias fueron diseñadas para ayudar a asegurar a América y su mundo cibernético mediante el establecimiento de tres objetivos principales: (1) Prevenir ataques cibernéticos contra la infraestructura crítica americana, (2) Reducir la vulnerabilidad nacional contra ataques cibernéticos, (3) Reducir los daños y recuperar el tiempo de ataques cibernéticos cuando estos ocurran.

La prioridad de la Estrategia Nacional para Asegurar el ciber-espacio es el establecimiento de un sistema de respuesta ciberespacial nacional. El DHS está en el proceso de perfeccionamiento de un sistema de respuesta, si un ataque cibernético grave ocurre. El plan también crea un sistema de seguridad contra una amenaza ciberespacial nacional, y reduce la vulnerabilidad del programa. Este programa haría un esfuerzo para identificar y castigar posibles atacantes, localizar y remediar sus vulnerabilidades existentes y desarrollar nuevos sistemas y tecnología que reduciría futuras vulnerabilidades.

[26] Ver la página de la Casa Blanca sobre The National Strategy to Secure Cyberspace. http://whitehouse.gov/pcipb.

The Critical Infrastructure Protection Act (CIPA) was enacted into law in 2002 to enhance the ability of the federal government to link with private industry in the sharing of information concerning previous Internet attacks. Under CIPA, information submitted to the government concerning a critical infrastructure program is exempt from disclosure under FOIA and may not be used by any government or third party in a civil action without the discloser's written consent.[27]

The Computer Fraud and Abuse Act (CFAA) prohibits accessing classified information unlawfully and damaging protected computers that results in physical injury, a threat to public health or safety, or damage to a computer used for national defense or national security. The CFAA expands the criminal penalties for such activities.

The Cyber Security Research and Development Act authorizes a multi-year effort to create more secure cyber technologies, to expand cyber security research and development, and to improve the workforce.[28]

For certain, when the West suffers its first "Pearl Harbor cyber attack," the government will implement programs to force private industry to share information and to develop better security systems. It is perhaps naive to place the burden for securing the nation's infrastructure on the shoulders of private industry - viable software to protect against cyber terrorism is not being fully pursued.[29] For now, apart from suffering economic loss itself, there are no driving incentives for private industry to work together to combat cyber terrorism. Still, given the expansion of the cyber world, there is no other option.

Indeed, there are several partnerships that are bearing fruit. One example is the Center for Infrastructure Assurance and Security (CIAS), located in San Antonio at the University of Texas at San Antonio. Among its many efforts to secure cyber space, in 2003 CIAS conducted the first large-scale cyber attack exercise since the terror attacks of September 11, 2001. Called, Dark Screen, the cyber exercise tested the ability of various government and business agencies to respond to attacks that affected the infrastructure, communication and information systems.[30]

[27] *But see* Brett Stohs, "Protecting the Homeland Exemption: Why the Critical Infrastructure Information Act of 2002 will Degrade the Freedom of Information Act," *Berkeley Technology Law Journal*, Summer 2003.
[28] Cyber Security Research and Development Act, PL 107-305.
[29] Ben Hunt, "Facing Up to the Threat from Cyber Terrorism," *Financial Times*, apr. 23, 2003 at 14.
[30] David McLemore, "On the Cyberterror Front Lines San Antonio Carving a Niche by Helping Protect Vital Systems," *Dallas Morning News*, sept. 21, 2003.

La Ley de Protección contra la Infraestructura Crítica (LPIC) fue decretada ley en el 2002 para mejorar la habilidad del gobierno federal de enlazarse con la industria privada compartiendo la información concerniente a previos ataques en Internet. Bajo la LPIC, la información sometida al gobierno concerniente al programa de infraestructura crítica está exenta de la divulgación bajo la LLI y puede no ser usada por ningún gobierno o un tercer partido en una acción civil sin el consentimiento escrito del divulgador[27].

La Ley Contra el Fraude y el Abuso de Computadores (LCFAC) prohíbe el acceso a información confidencial ilegalmente y el dañar computadores protegidos que resultasen en daño físico, una amenaza a la seguridad o a la salud pública, o el daño a un computador usado para la defensa nacional o la seguridad nacional. La LCFAC expande la pena criminal para dichas actividades.

La Ley de Desarrollo e Investigación en Seguridad Cibernética autoriza todo un año de esfuerzo para crear tecnologías cibernéticas más seguras, para expandir la investigación en seguridad cibernética, y así mejorar la fuerza de trabajo[28].

De seguro, cuando occidente sufra su primer "Peral Harbor cibernético", el gobierno implementará programas para forzar a la industria privada a compartir información y desarrollar mejores programas de seguridad. Tal vez, sea ingenuo colocar la carga en los hombros de la industria privada de asegurar la infraestructura de la nación y los programas de protección viables contra el terrorismo cibernético no están siendo completamente rastreados[29]. Por ahora, aparte de sufrir perdidas económicas, no hay incentivos que conduzcan a la industria privada a trabajar juntos y combatir el terrorismo cibernético. Aún, dándole la expansión al mundo cibernético, no hay otra opción.

Verdaderamente, varias sociedades están dando a luz. Un ejemplo en el Centro para el Aseguramiento de la Infraestructura y la seguridad (CAIS), localizada en San Antonio en la Universidad de Texas. Entre sus muchos esfuerzos para asegurar el ciber-espacio, en el 2003 el CAIS condujo un ejercicio el cual consistía en ser el primer ataque cibernético a gran escala desde el ataque terrorista del 11 de septiembre de 2001: Llamado *Pantalla Oscura*, el ejercicio cibernético examinó la habilidad de varios gobiernos y empresas para responder a ataques que afectan la infraestructura, las comunicaciones y los sistemas de información[30]

[27] Ver Brett Stosh, "Protecting the Homeland Exemption; Why the Critical Infrastructure Information Acto of 2002 will degrade the freedom of information Act, Berkeley Technology Law Journal, Summer, 2003
[28] Ver Cyber Security Research and Development Act, Pl 197-305.
[29] Ben Hunt, "Facing up to the Threat from Cyber Terrorism," Financial Times, apr. 23 at 14.
[30] David McLemore, "On the Cyberterror Front Lines San Antonio Carving a Niche By Helping Protect Vital Systems", Dallas Morning News, sept. 21,2003.

# IV. THE PATRIOT ACT AND COMBATING CYBER TERRORISM

Without question, the most well known piece of legislation associated with the terror attacks of september 11, 2001 is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," or more simply the Patriot Act.[31] Designed as a tool to assist law enforcement to disrupt terrorist cells and their base of operations, the Patriot Act was passed by an overwhelming majority of the Congress and signed into law by President Bush on October 26, 2001.[32]

The Patriot Act contains a mixed variety of criminal provisions aimed at both the investigation of suspected terrorists and disrupting the sources of funding and support for terrorist organizations. However, because almost all of the provisions in the Patriot Act amend or add language to existing federal statues, it is often difficult to encapsulate the full impact of many of the provisions at first glance. For example, §203 of the Patriot Act amends the Federal Rules of Criminal Procedure (FRCP)[33] to allow the sharing of grand jury information with other interested agencies if it relates to foreign intelligence; §219 of the Patriot Act amends the FRCP[34] to authorize nationwide search warrants for terrorism cases, and §213 of the Act adds a subsection to 18 U.S.C. §3103a in order to authorize a delayed notice of execution of a search warrant under specific conditions.

[31] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). The bill passed the Senate by a landslide vote of 98-1. 147 Cong. Rec. S11,059-60 (daily ed. Oct. 25, 2001). The House of Representatives passed their version by a similar lopsided vote of 357-66. 147 Cong. Rec. H7224 (daily ed. Oct. 25, 2001). *See also*, Electronic Privacy Information Center Web site on the USA Patriot Act, http://www.epic.org/privacy/terrorism/usapatriot/.

[32] *Id.*

[33] FRCP 6(e)(3)(C).

[34] FRCP 41(a).

# IV. LA LEY PATRIOTA Y EL COMBATE CONTRA EL TERRORISMO CIBERNÉTICO

Sin lugar a dudas, la más conocida pieza de legislación asociada con los ataques terroristas de septiembre de 2001 es la "ley del 2001 de Unificación, Fortalecimiento de América mediante el Abastecimiento Apropiado de Herramientas Requeridas para Interceptar y Obstruir el Terrorismo", o más simple: "La Ley Patriota"[31]. Diseñada como herramienta para asistir la aplicación de la ley para dividir a las células terroristas y sus bases de operación, la Ley Patriota fue aprobada por una mayoría abrumadora del Congreso y firmada legalmente por el presidente Bush el 26 de octubre de 2001[32].

La Ley Patriota contiene una variedad mezclada de previsiones criminales enfocadas a la investigación de terroristas sospechosos y a dividir las fuentes de financiamiento y apoyo de las organizaciones terroristas. Sin embargo, debido a que casi todas las previsiones en la Ley Patriota corrigen o añaden lenguaje de estatus federal ya existentes, a menudo encapsular todo el impacto de muchas previsiones al primer vistazo. Por ejemplo, la enmienda 203 de la Ley Patriota, Las reglas Federales del Procedimiento Criminal (RFPC)[33] para permitir compartir con el gran jurado información con otras agencias interesadas; la enmienda 219 de la Ley Patriota, al RFPC[34] autorizó órdenes de captura a lo largo del territorio para casos de terrorismo y la enmienda 213 de la ley añade una subsección a la enmienda 3103 para autorizar una nota retrasada de ejecución de la orden de captura bajo condiciones específicas.

[31] La ley fue pasada al Senado y ganó por mayoría; de 98-1. 147 Cong. Rec. S11, 059-60 (daily ed. oct.25,/01) La Casa de Representantes paso su versión por una votación similar 357-66. 147 Cong. Rec. H7224 (daily ed. Oct 25/ 01).
Ver, también Electronic Privacy Information Center Web site on the USA Patriot Act, http://www.epic.org/privacy/terrorism/usapatriot/.

[32] Id.

[33] FRCP 6(e)(3)(c)

[34] FRCP 41 (a)

In terms of cyber terrorism, a number of legislative changes were instituted that expanded the ability of both law enforcement and intelligence agencies regarding surveillance and investigative powers. To be sure, the Patriot Act allows federal authorities far greater freedom in monitoring the Internet and provides for a streamlined system of sharing gathered information with other federal and State agencies. Other important tools are found in the ability of law enforcement agents to employ "pen registers;" "trap and trace" devices; "sneak and peak" searches; and "roving wiretaps," which permits surveillance on the person and not, for example, on the phone or phone number. §814 of the Patriot Act is entitled: "Pen Register and Trap and Trace Authority under FISA." This section expands the scope of the Foreign Intelligence Surveillance Act of 1978 (FISA) and provides greater powers to the FISA courts to grant court orders for surveillance.

In addition, both the Patriot Act at §214 and the Cyber Security and Enhancement Act (CSEA) have eased the warrant and subpoena requirements under the old Electric Communications Privacy Act of 1986 (ECPA). Under the CSEA (which amends certain sections of Title 18 of the United States Code), the government official need not obtain a warrant of subpoena if he has a "good faith" belief regarding the prevention of death or serious bodily harm. In addition, the CSEA amends 18 U.S.C. §3125(a)(1) to allow a government official to use a pen register or a trap and trace device without a warrant or a court order if there is a "threat to national security and an ongoing attack on a protected computer system."[35]

In traditional terms, a pen register is simply a process that collects the outgoing phone numbers from a specific telephone line, while a trap and trace device captures the incoming numbers placed to a specific phone or computer line.[36] Prior to the enactment of the Patriot Act, pen registers and trap devices could only be used to intercept the numbers dialed or transmitted on the telephone line that was specifically attached to the device. In addition, the old statutory language limited the use of such devises to telephone lines. Understanding the fantastic growth in electronic devices used to communicate information, the Patriot Act redefined pen register to mean "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[37]

[35] The Homeland Security Act of 2002, PL 107-298, 116 Stat 2135 (nov. 24, 2002).
[36] *See* the Electronic Privacy Information Center Web site on the USA Patriot Act. http://www.epic.org/privacy/terrorism/usapatriot/.
[37] *Id.*

En términos de terrorismo cibernético, un sin número de cambios legislativos fueron instituidos, ampliando la habilidad de la aplicación de la ley y las agencias de inteligencia en lo que tiene que ver con vigilancia y poderes investigativos. Para estar seguros, la Ley Patriota le permite a las autoridades federales muchas más libertades para monitorear Internet y de proveer un sistema aerodinámico de compartir información reunida con otras agencias federales y estatales. Otras herramientas importantes se encuentran en la habilidad de los agentes para la aplicación de la ley y emplear "registros escritos", artefactos de "trampas y rastreo", las cuales permiten vigilancia sobre la persona y no, por ejemplo, en el teléfono o en el número telefónico. La enmienda 814 de la Ley Patriota es titulada: "Autoridad de Registro, Trampa y Rastreo" bajo la LVIE. Esta sección amplia el radio de acción de la LVIE (Ley de Vigilancia de Inteligencia Extranjera de 1978) y provee mayores poderes a la corte de la LVIE otorgando a las grandes cortes órdenes de vigilancia.[35]

Además, tanto la Ley Patriota 214 y la Ley de Seguridad Cibernética y de Perfeccionamiento han facilitado la garantía y los requerimientos de citación bajo la vieja Ley de Comunicación Eléctrica Privada de 1986, un oficial de gobierno no necesita obtener una orden de captura si él cree poder prevenir la muerte o el maltrato físico. Además, la enmienda 3125 le permite a un oficial del gobierno utilizar un registro escrito o un artefacto de trampa y rastreo sin una orden, "si hay una amenaza a la seguridad de la nación o si está sucediendo un ataque en un sistema de computadores protegidos".

En términos tradicionales, un registro escrito es simplemente un proceso que recolecta los salientes números telefónicos de una línea específica[36], mientras que un artefacto con trampa captura los números entrantes colocados en un número específico o en una línea de computador. Anteriormente a la norma de la Ley Patriota, los registros escritos y los artefactos con trampas solo podían ser utilizados para interceptar números marcados o trasmitidos en las líneas telefónicas que estaban específicamente adheridas al artefacto. Además, el viejo lenguaje estatutario limitaba el uso de tales artefactos a las líneas telefónicas. Entendiendo el fantástico crecimiento de los artefactos electrónicos[37] y su uso en la comunicación de la información, la Ley Patriota redefine registro escrito al significado de: dirigir o transmitir señales de información por medio de un instrumento o un establecimiento desde donde un cable o una comunicación electrónica es trasmitida.

[35] The Homeland Security Acto f 2002, PL 107-298, 116 Stat 2135 (nov. 24, 2002).
[36] Ver The Electronic Privacy Information Center Web site on the USA Patriot Act. http://www.epic.org/privacy/terrorism/usapatriot/.
[37] Id.

In short, the use of pen registers under the Patriot Act now allows for the tapping of all sorts of private activity on the Internet and allows law enforcement to collect private information communicated even from personal e-mails. A pen register and trap and trace device that is used in association with the Internet allows federal agencies to capture all the email headers going to and from an email account, list all servers that a suspect accesses, track anyone that accesses a certain web page, and track all web pages that a particular suspect may access.[38] Thus, armed with the new definitions, pen registers and trap and trace now allow federal agencies to include not only telephone lines, but also the Internet, electronic mail, Web surfing, and any other form of electronic communication. Although the law prohibits the collection of "content," this can be an ambiguous term - valuable data can still be collected that is more personal than a home telephone number.

Pen registers are also used in conjunction with a program initially known as "Carnivore" but now called DCS-1000. DCS-1000 is an Internet surveillance program developed by the FBI that allows federal law enforcement, in cooperation with an Internet Service Provider, to carry out court orders for the collection of certain information contained in emails and other electronic communication to or from a specific user.[39] Internet communications are filtered to select a suspect's email. The DCS-1000 can be plugged into an Internet Service Provider's network, allowing the software to monitor the routing information for billions of emails and to make copies of emails from particular suspects. While the FBI will not reveal the specifics of how this software functions, depending on the court's direction or limitation DCS-1000 can be tailored to only record the email itself and not the text.

[38] *Id.*
[39] *See* Electronic Privacy Information Center Web site on the Carnivore System, http://www.epic.org/privacy/carnivore.

Para abreviar, el uso de los registros escritos bajo la Ley Patriota ahora permite grabar toda clase de actividades privadas en Internet y permite la aplicación de la ley para recolectar información privada comunicada hasta de correos electrónicos personales. El registro escrito y el artefacto de trampa y rastreo que es utilizado en asociación con Internet le permite a las agencias federales capturar todos los correos electrónicos dirigidos de una cuenta electrónica, hacer una lista de todos los servidores a los cuales algún sospechoso tenga acceso, rastrear cualquiera que tenga acceso a una determinada página web, y rastrear todas las páginas web a las cuales un sospechoso en particular pueda tener acceso[38]. Así, armados con las nuevas definiciones, los registros escritos y los artefactos de trampa y rastreo ahora le permiten a las agencias federales incluir no sólo líneas telefónicas, sino también Internet, correos electrónicos, navegar la red y cualquier otra forma de información electrónica. Aunque, la ley prohíbe la recolección de "contenido" esto puede ser un término ambiguo, información con valor puede todavía ser recolectada, lo cual, es más personal que un número telefónico.

Los registros escritos también son usados en conjunción con un programa inicial conocido como "carnívoro", ahora llamado "DCS-1000" el cual es un programa de vigilancia de Internet desarrollado por el FBI que permite la aplicación de las leyes federales, en cooperación con los servidores de Internet, para llevar acabo órdenes judiciales para la recolección de cierta información contenida en correos electrónicos y otras comunicaciones electrónicas que lleguen o salgan de un usuario determinado[39]. Las comunicaciones de Internet filtradas para seleccionar un sospechoso en la red. El DCS-1000 puede ser conectado en un servidor de red, permitiéndole al programa monitorear la información dirigida a través de billones de correos electrónicos y de hacer copias de correos electrónicos de sospechosos en particular. Mientras el FBI no revele las partes especificas de cómo este programa funciona, dependiendo de la dirección o limitaciones de la corte, el DCS-1000 puede ser diseñado sólo para grabar el mismo correo electrónico y no el texto.

[38] Id.
[39] Ver Electronic Privacy Information Cen er Web site on the Carnivore System, htpp://www.epic.org/privacy/carnivore.

DCS-1000 technology provides federal law enforcement far greater surveillance latitude in monitoring possible terrorist organizations that are located in the United Sates as well as in foreign countries. In this manner, the FBI is able to track communications between terrorist cells that often do much of their communicating and recruitment through the Internet and other electronic transmissions. Monitoring this type of information is a much needed anti-terrorist tool to prevent attacks on other computer networking systems. John Pistole, FBI terrorism chief, noted that "focusing on intelligence gathering will improve the ability of the FBI to prevent, rather than just investigate terrorist attacks."[40]

In the realm of obtaining search warrants for electronic surveillance, one area of concern for law enforcement prior to the Patriot Act dealt with complying with the extremely narrow constraints set out by 28 U.S.C. §2510, known as Title III. Title III sets out a strict limit regarding the issuance of search warrants for any form of electronic surveillance that exceeds a reasonable expectation of privacy and applied those limits to the federal and State level at any type of court proceeding (administrative, criminal, or civil). Although Title III does not extend to video surveillance it covers all "wire, oral or electronic communications" to include electronic mail, computer-to-computer communications, cellular telephones, etc. Under Title III, the warrant issued by the proper district or appellant federal judge (or State equivalent) must:

- Identify the applicant.
- Detail the suspected criminal offenses.
- Detail the facilities to be used, the types of communications to be intercepted, and the identity of the person whose conversation is to be intercepted.
- A description of other *less intrusive means* to get the information and why they have failed or would likely fail. The judge issuing the warrant will list why normal procedures are inadequate.
- Detail the time frame of the surveillance.
- List any previous applications for the same surveillance.

Title III does contain an "emergency" provision that allows for a warrantless electronic surveillance in cases involving conspiratorial activities threatening national security, organized crime, or instances of immediate danger of death or serious physical harm to any person.[41] However, unless one of the very limited exceptions applies, Title III prohibits the intentional interception or disclosure of contents of any intercepted communications without properly complying with the requirements of the wiretap statute.

The Patriot Act expands the list of previous exceptions in Title III to include "government interception of the communications of a computer trespasser if the owner or operator of a 'protected computer' authorizes the interception." In turn, a "protected computer" is defined as one that is used in interstate or foreign commerce or communication. Indeed, given the limitless boundaries of the information super highway, that definition could apply to virtually every computer. Thus, if the system owner gives his authorization, federal authorities are allowed to wiretap and investigate the communication without the need for the rigid judicial oversight set out in Title III. For example, this provision now allows a business owner of a system that has been the target of a terrorist "hack" to authorize a wiretap without judicial oversight. Any information that is gleaned from that wiretap can be used in a subsequent criminal investigation. Clearly, this ability to bypass Title III is a significant tool in helping prevent cyber attacks. Federal agencies can now use the information created by a computer trespasser to locate other possible targets of the hacker and thereby prevent future attacks.

One of the most controversial provisions of the Patriot Act is §213, which grants federal agencies the ability to conduct secret searches when armed with the appropriate probable cause judicial warrant. "Section 213 of the USA Patriot Act eliminates the prior requirement that law enforcement provide a person subject to a search warrant with contemporaneous notice of the search."[42]

---

[40] *See* Dan Eggen, "FBI Applies New Rules to Surveillance," *Washingtonpost.com*, december 13, 2003.
[41] Title III, § 2518(7).
[42] *Id.*

La tecnología del DCS-1000 provee la aplicación de la ley federal con una mayor vigilancia a nivel de latitud y monitorear posibles organizaciones terroristas que estén ubicadas en los Estados Unidos como también en otros países extranjeros. De esta manera, el FBI es capaz de monitorear las comunicaciones entre células terroristas y a menudo se comunican y se reclutan a través de Internet y otros medios electrónicos. El monitoreo de clase de información, una herramienta antiterrorista más necesaria para prevenir ataques en otros sistemas de red de computadores. John Pistole, jefe de terrorismo del FBI, notó que "el enfoque sobre inteligencia agrupada mejorará la habilidad del FBI para prevenir en vez de sólo investigar ataques terroristas"[40]

En el área para obtener órdenes de captura para la vigilancia electrónica, un área de interés para la aplicación de la ley anterior a la Ley Patriota tiene que ver con el cumplimiento de las extremadamente estrechas restricciones emprendidas por la enmienda 2510, conocida como Título III. El Título III emprende un límite estricto en cuanto a la expedición de órdenes de captura para cualquier forma electrónica de vigilancia que exceda una expectativa razonable de privacidad y aplicar esos límites al nivel del Estado federal y cualquier tipo de procedimiento judicial (administrativo, criminal o civil). Aunque, el Título III no se extiende a la video vigilancia, esta cubre todo "comunicaciones orales, por cable o electrónicas", incluyendo correos electrónicos, comunicaciones de computador a computador, teléfonos, celulares. Bajo el Título III, la emisión de órdenes de captura por el debido distrito o juez federal apelante (o estado equivalente) debe:

- Identificar el candidato.
- Detallar las ofensas del criminal sospechoso.
- Detallar las instalaciones a usar, tipos de comunicación a ser interceptados y la identidad de la persona a quién se va a interceptar la comunicación.
- Una descripción de unos medios menos invasivos para obtener información y por qué ellos han fallado o por qué fallarían. El juez que emite la orden de captura haría una lista del por qué los procedimientos normales son inadecuados.
- Detallar el tiempo y el marco de vigilancia.
- Hacer un listado de los formatos anteriores de registro para la misma vigilancia.

El Título contiene una provisión de "emergencia" que permite una vigilancia electrónica sin una orden judicial en casos que involucren conspiraciones que amenacen la seguridad nacional, el crimen organizado o instancia de peligro inmediato de muerte o serio daño físico a cualquier persona[41].Sin embargo, a no ser que unas excepciones muy limitadas apliquen, el Título III prohibe la intercepción intencional o la divulgación del contenido de cualquier comunicación interceptada sin el cumplimiento debido de acuerdo a los requerimientos del estatuto de rastreo.

La Ley Patriota extiende la lista de excepciones previas en el Título III incluyendo "la intercepción del gobierno de comunicaciones de un computador protegido autoriza la intercepción", a su vez, un computador "protegido" es definido como uno que es usado dentro del estado o comercio extranjero o comunicación. Verdaderamente, dando una frontera sin límites de la gran autopista de la información, esa definición podría aplicar virtualmente a cualquier computador. De esta manera, si el dueño del computador da la autorización, las autoridades federales tiene permiso de rastrear e investigar la comunicación sin necesidad de vigilancia judicial rígida, partiendo del Título III. Por ejemplo, esta provisión permite a los dueños de las compañías de un sistema que ha sido el blanco de un ataque terrorista "hack" autorizar el rastreo sin vigilancia judicial. Cualquier información que esté fraccionada del rastreo puede ser utilizada en una investigación criminal subsiguiente. Claramente, esta habilidad de desviar el Título III es una herramienta significativa para ayudar a prevenir ataques cibernéticos. Las agencias federales ahora pueden utilizar la información creada por un computador intruso para localizar otros posibles blancos del hacker y, por lo tanto, prevenir ataques futuros.

Una de las previsiones más controversiales de la Ley Patriota es la enmienda 213 la cual otorga a las agencias federales la habilidad para conducir investigaciones secretas cuando estén con la apropiada orden judicial de la probable causa. "la sección 213 de la Ley Patriota americana elimina los requerimientos previos que la aplicación que la ley provee a una persona sujeta a orden de captura con notificación contemporánea a la búsqueda"[42]

[40] Ver Dan Eggen, "FBI Applies New Rules to Surveillance", Washingtonpost.com, december 13,2003
[41] Título III §2518 (7)
[42] Id.

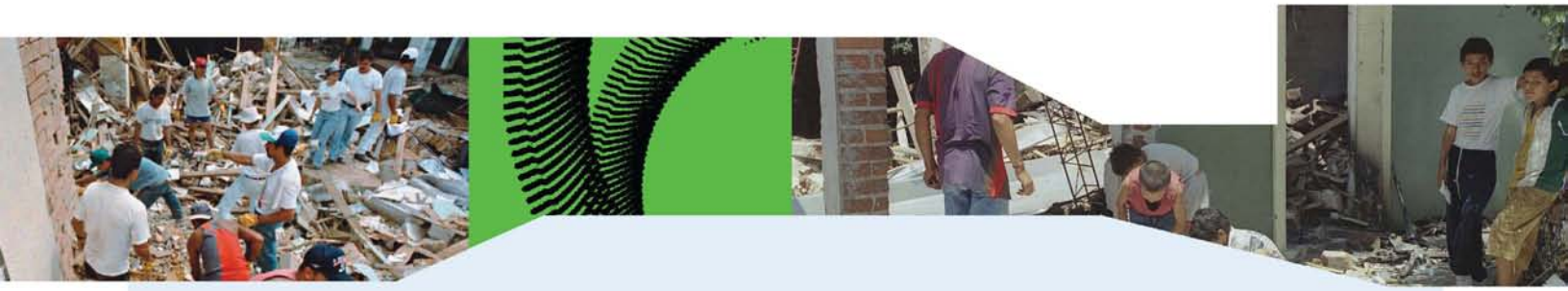
Known as sneak and peak, these searches allow law enforcement officers the authority to search and seize any tangible object or record without notification to the owner or possessor when the court finds "reasonable necessity" for action. Although no time limit is established for when the subject must be notified, case law would suggest that it is a matter of days and not weeks.

Sneak and peak authority has stirred debates over the provision's value to the defense of the nation and its attendant harm to civil liberties. Representative C.L. "Butch" Ottor, (R-Idaho), offered his view at a floor debate: "Sneak-and-peak searches give the government the power to repeatedly search a private residence without informing the residents that he or she is the target of an investigation. Not only does this provision allow the seizure of personal property and business records without notification, but it also opens the door to nationwide search warrants and allows the CIA and the NSA [National Security Agency] to operate domestically."[43]

Despite the rhetoric, sneak and peak searches cannot be carried out without a court order issued by a neutral and detached magistrate. In addition, in order to perform this type of search the court must find "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse effect" on the investigation.[44] The law does not allow for searches to be committed without any notification, it simply allows for a delay in notification when there is reasonable belief that prior notification could damage the investigation.

Obviously, the sneak and peak provision is an extremely valuable tool because it allows the authorities to gather evidence without "tipping their hand." Often many terrorists, or groups of terrorists in "sleeper cells," maintain only temporary domiciles and are known to move locations very quickly. This provision aids officials in gathering valuable information from a suspect's house without alerting the suspect of the investigation.

[43] *See* Dan Eggen, "FBI Applies New Rules to Surveillance," *Washingtonpost.com*, december 13, 2003.
[44] *Id.*



Estas búsquedas permiten a los oficiales que aplican la ley, tener la autoridad para buscar y confiscar cualquier objeto tangible o de grabar sin notificar al dueño cuando la corte encuentre "la necesidad razonable" para tal acción. Aunque, no hay tiempo limite para que el sujeto sea notificado, el caso legal sugeriría que es cuestión de días y no de semanas.

Las autoridades han debatido sobre la provisión de valor a la defensa de la nación y su acompañamiento dañino contra la libertad civil. El representante C.L. "Butch" Ottor (R Idazo), ofreció darle un vistazo al debate; "las investigaciones de rastreo le dan al gobierno el poder de investigar repetidamente una residencia privada sin informar a sus residentes que él o ella son el blanco de la investigación". "Esta provisión, no sólo permite la confiscación de la propiedad personal y la información de la compañía sin notificación, sino también abre la puerta a órdenes de captura a lo largo de la nación y le da a la CIA y a la ANS (Agencia Nacional de Seguridad) operar domésticamente[43].

A pesar de la retórica, las investigaciones de rastreo no pueden ser llevadas a cado sin la expedición de una orden judicial por un magistrado neutral o aislado. Además, para desarrollar esta clase de investigación la corte debe encontrar "una causa razonable para creer que sustentando una notificación inmediata de la ejecución de la orden pueda tener un efecto contrario" en la investigación[44]. La ley no permite investigaciones a seguir sin ninguna notificación, solo permite una notificación retrasada cuando hay una creencia razonable que antes de la notificación pudiera dañar la investigación.

Obviamente, la provisión del rastreo es una herramienta valiosa porque permite a las autoridades reunir información sin "encintarse las manos". A menudo, algunos terroristas, o grupos terroristas "en células durmientes" mantienen solo domicilios temporales y se conoce que cambian de locución muy rápido. Esta provisión auxilia a los oficiales para recoger valiosa información de la casa del sospechoso sin alterar la investigación.

[43] Ver Dan Eggen, , "FBI Applies New Rules to Surveillance", Washingtonpost.com, december 13,2003
[44] Id.

In this context, the property that could possibly be seized (or copied) could include laptop computers and other computer records. Assistant Attorney General, William Moschella claims that a "terrorist would likely destroy computer equipment containing information about which targets he plans to strike," but the secret searches could help prevent that from happening.[45]

The expansion of the roving wiretap by the Patriot Act permits the interception of any communications made to or by a suspect without identifying a specific telephone line or computer system to be monitored. Furthermore, the Patriot Act changes the original law which required that third parties, such as common carriers, be specified in a court order before they could provide assistance in the surveillance. The new law extends that obligation to any unnamed and unspecified third party. Those parties would include, for instance, any libraries that provide Internet access, university computer labs, and Internet cafes. This allows federal agencies the ability to monitor these facilities if they have probable cause to believe that a terrorist or intelligence target is using the facility to transmit communications.

The Patriot Act also allows the government to administratively detain suspected terrorists who are illegal aliens. Specifically, §412(a) of the Patriot Act adds §236A to the Immigration and Nationality Act,[46] allowing the Attorney General to take into custody any alien *certified* to be inadmissible or deportable on one of six grounds: (1) espionage, (2) sabotage, (3) export restrictions, (4) attempt to overthrow the U.S. Government; (5) terrorist activities, and (6) any other "activity that endangers the national security of the United States."[47] Section 412(a)(5) then requires the government to either begin criminal or deportation proceedings within seven days of the detention.[48] Ostensibly, however, §412(a)(6) empowers the government to indefinitely detain certain certified illegal alien terrorists who are not likely to be deported in the foreseeable future due to the continuing nature of the investigation.[49]

[45] *Id.*
[46] Immigration and Nationality Act, 8 U.S.C. § 1001 et seq. The changes codified as 8 U.S.C. § 1226A.
[47] *Id.* at (3).
[48] *Id.* at (5).
[49] Immigration and Nationality Act, 8 U.S.C. § 1001 et seq. The changes codified as 8 U.S.C. § 1226A(6).

En este contexto, la propiedad que puede ser allanada, podría incluir computadores portátiles y otros archivos del computador. El abogado general, William Moschella afirma que "un terrorista probablemente destruiría un equipo que contiene información sobre los blancos que piensa atacar", pero las investigaciones secretas podrían ayudar a prevenir que eso suceda[45].

La expansión del rastreo por medio de la Ley Patriota permite la intercepción de cualquier comunicación hecha a un o por un sospechoso sin identificar una línea telefónica específica o algún sistema computarizado a ser monitoreado. Además, la Ley Patriota cambia la ley original, la cual requiere que terceros, tales como portadores comunes, sean especificados en un tribunal antes que ellos pudieran proveer ayuda en la vigilancia. La nueva ley extiende esa obligación a cualquier tercer partido sin nombrar ni especificar. Esos terceros incluirían, por ejemplo, cualquier biblioteca que provea acceso a Internet, universidades con laboratorio de computadores, y cafés Internet. Esto le permite a las agencias federales la habilidad de monitorear esos centros si ellos tienen alguna causa probable para creer que un terrorista o un blanco de inteligencia está usando el centro para transmitir comunicaciones.

La Ley Patriota también permite al gobierno administrativamente detener terroristas sospechosos que sean extranjeros ilegales. Específicamente, la enmienda 412 (a) de la Ley Patriota y la enmienda 236 (a) de la Ley de Nacionalidad e Inmigración[46], permite al abogado general tomar en custodia cualquier extranjero certificado como inadmisible o deportable en uno de los seis campos: (1) espionaje, (2) sabotaje, (3) restricciones para exportar, (4) intento de derrocar al gobierno americano, (5) actividades terroristas, (6) cualquier otra "actividad que ponga en peligro la seguridad nacional de los Estados Unidos"[47]. Entonces, la sección 412 (a) (5) requiere del gobierno ya sea empezar procedimientos criminales o de deportación dentro de los siete días de la detención[48]. Sin embargo, ostensiblemente, la enmienda 412 (a) (6) le da poder al gobierno para detener indefinidamente un determinado extranjero ilegal terrorista, el cual, posiblemente, no sea deportado en el futuro previsible debido a la naturaleza continua de la investigación[49].

[45] Id.
[46] Immigration and Nationality Act, 8 U.S.U. § 1001 et seq. The changes codified as 8 U.S.U. §1226 A.
[47] Id. At (3)
[48] Id. At(5)
[49] Immigration and Nationality Act, 8 U.S.U. § 1001 et seq. The changes codified as 8 U.S.U. §1226 A.

The question of concern regards the matter how long a certified individual terrorist may be detained and under what conditions?[50] While the U.S. Supreme Court has yet to rule on the constitutionality of §412(a)(6), its decision in Zadvydas v. Davis[51] means that it will probably find that §412(a)(6) is constitutional. Zadvydas seemingly exempted suspected alien terrorists as a "small segment of particularly dangerous individuals" that the government could subject to indefinite detention.[52]

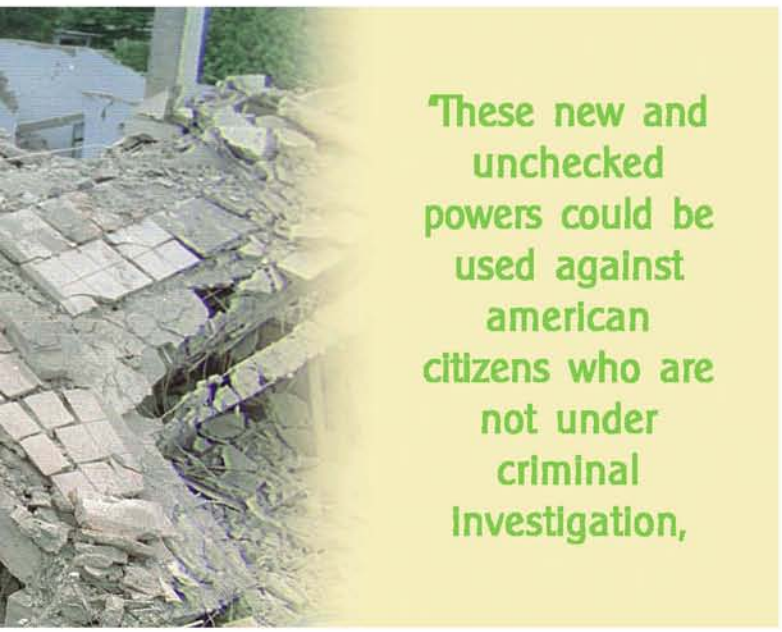
The Patriot Act's provisions on indefinite detention for certified detainees is likely to pass constitutional muster because it actually exceeds the Zadvydas standard regarding suspected terrorists held on an indefinite basis. First, §412(b) specifically provides that judicial review of detentions of suspected alien terrorists is via habeas corpus.[53] Second, the new law proscribes fixed time limits for review of the Attorney General's certification. §412(a)(6) provides that an alien whose "removal is unlikely in the reasonably foreseeable future, may be detained for additional periods of up to six months if release threatens national security or the safety of an individual or the community."[54] Furthermore, §412(a)(7) requires the Attorney General to review said certification every six months and allows the suspected illegal alien terrorist to request a reconsideration of the certification every six months.[55] If these provisions are satisfied, the said terrorist suspect may be held indefinitely.

In summary, the basic provisions set out in this monograph compliment other new law enforcement tools defined in the Patriot Act, e.g., the detention of illegal aliens suspected of being terrorists, and combine to give the intelligence and law enforcement agencies greater access to track down terrorists and help prevent future attacks. Such changes have proved to be instrumental, allowing the FBI to disrupt plans for numerous terrorist attacks overseas and uncover sleeper cells in the United States.

To even the cursory viewer, the advances in technology have caused a shift in law enforcement techniques that are stretching the protections of the Constitution's 4th Amendment (unreasonable searches and seizures). For example, one area that is not covered in the Patriot Act involves the question of whether law enforcement should be able to unscramble an encrypted communication back into a readable form. It is common knowledge that sophisticated terrorists are now using cloaking devices provided by encryption companies to keep police from reading their communications. Thus, even if law enforcement can intercept the scrambled communications sent by terror suspects, they have no way of translating the information back into readable form. Consequently, legislation is probably necessary to more fully force encryption companies to provide a "back door" to allow law enforcement agencies access.

Interestingly, there are many who object to the Patriot Act as a violation of civil liberties. According to Gregory Nojeim, the Associate Director of the ACLU's Washington Office: "These new and unchecked powers could be used against American citizens who are not under criminal investigation, immigrants who are here within our borders legally and also those whose First Amendment activities are deemed to be threats to national security by the Attorney General."[56]

A handful of States and many local governments around the nation have expressed opposition to the Patriot Act in the form of resolutions or even local statutes. In February 2004, the city of New York approved a resolution condemning the Patriot Act. In doing so, New York City joined 246 other municipalities and counties, along with three States that have enacted legislation in opposition to the Patriot Act. One New York City council member spoke out about the new measure stating: "The Patriot Act is really unpatriotic, it undermines our civil rights and civil liberties."[57]



"These new and unchecked powers could be used against american citizens who are not under criminal investigation,

[50] A collateral question also arises in terms of the Attorney General's power to determine who qualifies is a terrorist. This question will certainly be argued along the lines of how much deference is given by the Courts to the political branches in matters of national security. *See, e.g.*, Cooler & Gell v. Hartmarz Corp., 496 U.S. 384, 400 (1990).

[51] Zadvydas v. Davis, 121 S. Ct. 2491 (2001). The Court in Zadvydas did recognize in the opinion that suspected terrorists could be held for indefinite periods in preventive detention. The Court understood that illegal aliens detained for "terrorism or other special circumstances where special arguments might be made for forms of preventive detention," should not be affected by the general rule disapproving the indefinite detention of resident aliens not likely to be deported.

[52] *Id.* at 2499.

[53] 8 U.S.C.§ 1126B. Actually, the section limits judicial review to habeas corpus without providing for a standard of review.

[54] 8 U.S.C.§ 1126A(6)

[55] *Id.* at (7).

[56] *See* Stefanie Olson, "Patriot Act Draws Privacy Concerns," *CNET News.com*, October 26, 2001.

[57] *See* Michelle Garcia, "N.Y. City Council Passes Anti-Patriot Act Measure," *Washingtonpost.com*, february 5, 2004, at A11.

La cuestión esencial es ¿cuánto tiempo un terrorista certificado puede ser detenido y bajo qué condiciones?[50] Miestras que la Corte Suprema de los Estados Unidos aún tiene que fallar sobre la constitucionalidad de la emnienta 412 (a) (6), su desición en Zadvydas V. Davis[51] significa que probablemente encontrará que la enmienda 412(a)(6) es constitucional. Aparentemente, Zadvydas, extranjero, eximido de ser sospechoso terrorista como"un segmento particularmente pequeño de individuos peligrosos" que el gobierno podría someter a detención indefinida[52].

Las provisiones de la Ley Patriota en cuanto a la detención indefinida para detenidos certificados es probable que sea aprobada constitucionalmente, porque actualmente excede los estándares de Zadvydas con respecto a supuestos terroristas cautivos bajo bases indefinidas. Primero, la enmienda 412(b), específicamente que provee una revisión judicial sobre las detenciones de extranjeros terroristas sospechosos está en *vía habeas corpus*[53]. Segundo, la nueva ley proscribe el tiempo limite reparado para revisar la certificación del Abogado General. La enmienda 412(a)(6) provee que un extranjero, el cual "su liberación sea improbable en un futuro previsible razonable, pueda ser detenido por períodos adicionales de más de seis meses si su liberación amenaza la seguridad nacional o la seguridad de un individuo o la misma comunidad"[54]. Además, la enmienda 412(a)(7) requiere que el abogado general revise dicha certificación cada seis meses y permita al extranjero ilegal supuestamente terrorista a pedir una reconsideración de la certificación cada seis meses[55]. Si estas provisiones son satisfechas, el dicho supuesto terrorista puede permanecer cautivo indefinidamente.

En resumen, las provisiones básicas que emprenden esta monografía alaban otras nuevas herramientas para la aplicación de la ley definidas en la Ley Patriota, por ejemplo: la detención de extranjeros ilegales supuestamente terroristas, y combina los agentes de inteligencia y a las agencias para aplicar la ley y tener mayor acceso para rastrear terroristas y evitar futuros ataques. Tales cambios han demostrado ser instrumentos, que le permiten al FBI romper los planes de un sin número de ataques terroristas en el extranjero y de descubrir células terroristas durmientes en los Estados Unidos.

Hasta para el observador superficial, los avances en la tecnología han causado un cambio en las técnicas de aplicación de la ley que están estirando la protección del cuarto estatuto de la constitución (búsquedas y allanamientos no razonables). Por ejemplo, un área que no está cubierta en la Ley Patriota involucra la pregunta si la aplicación de la ley deba ser capaz de descifrar una comunicación encriptada y convertirla en una forma leíble. Es de conocimiento común que los terroristas sofisticados ahora están usando artefactos encubiertos provistos por

"Este nuevo poder desenfrenado puede ser utilizado contra ciudadanos americanos quienes no están bajo una investigación criminal...

compañías encriptadas para evitar que la policía lea sus comunicaciones. Aunque, si la aplicación de la ley puede interceptar la comunicación revuelta enviada por supuestos terroristas, ellos no tienen forma de traducir la información de una forma leíble. Consecuentemente, es probable que sea necesaria la legislación para forzar más a las compañías encriptadas a proveer una "puerta trasera" para permitir el acceso a la aplicación de la ley.

Interesantemente, hay muchos que objetan la Ley Patriota como una violación a las libertades civiles. De acuerdo a Gregory Nojeim, el Director Asociado de la ACLU de la oficina de Washington: "Este nuevo poder desenfrenado puede ser utilizado contra ciudadanos americanos quienes no están bajo una investigación criminal, inmigrantes quienes están aquí, dentro de nuestras fronteras legales y también aquellos que sus primeras actividades de enmienda se cree que son amenazas a la seguridad nacional según el Abogado General"[56].

Un puñado de Estados y varios gobiernos locales al rededor de la nación han expresado oposición a la Ley Patriota en la forma de las resoluciones o inclusive estatutos locales. En febrero del 2004, la ciudad de New York aprobó la resolución condenando la Ley Patriota. De tal manera, la ciudad de New York se unió a 246 municipios y condados, junto con tres Estados que habían decretado legislación en oposición a la Ley Patriota. Un miembro del concejo de New York habló sobre la nueva medida: "la Ley Patriota es realmente antipatriota, esta socava nuestros derechos civiles y nuestras libertades civiles"[57].

---

[50] También surge una pregunta colateral en términos del poder del Fiscal para determinar quién cualifica el término "terrorista". Esta pregunta seguramente será discutida a lo largo de las líneas de cuanta deferencia se le da por las cortes y a las ramas políticas en materia de seguridad nacional. Ver. Cooler & Gell v. Hartmarz Corp. 496 U.S. 384, 400 (1990)

[51] Zadvydas v. Davis 121 S.Ct.2491 (2001). La Corte en Zadvydas realmente reconoció a la opinión que los supuestos terroristas podrían permanecer en la cárcel por períodos indefinidos como detención preventiva. La Corte entendió que los ciudadanos extranjeros detenidos por terrorismo u otra circunstancia especial donde los argumentos especiales podrían estar hechos como formas de detención preventiva, y no deberían afectarse por la norma general de desaprobar la detención preventiva para ciudadanos extranjeros que no se asemejen a una deportación.

[52] USA. . 1126. Actualmente, la sección limita el repaso judicial debido a un habeas corpus sin proveer alguna revisión Standard.

[53] USA .C. 1126 A (6 )

[54] Id. At (7)

[55] *Id.* at (7).

[56] *Ver* Stefanie Olson, "Patriot Act Draws Privacy Concerns," *CNET News.com*, octubre 26, 2001.

[57] *Ver* Michelle Garcia, "N.Y. City Council Passes Anti-Patriot Act Measure," *Washingtonpost.com*, febrero 5, 2004, at A11.

Despite efforts to "demonize" the Patriot Act, the provisions are actually a judicious effort to stop future terror attacks, particularly in the realm of cyber terrorism. Commenting on the number of local governments that had passed resolutions or laws against the Patriot Act, a Justice Department spokesman noted that many of the ordinances were based on "erroneous" information about the Act and that the Patriot Act "has been one of the most important tools Congress has given the government to fight terrorism and prevent terrorist attacks."[58] In fact, many provisions in the Patriot Act speak to the issues of due process concerns. For example, §214 of the Patriot Act states that a FISA court order should not authorize the gathering of foreign intelligence information for an investigation concerning a United States person or surveillance when the person has been singled out solely upon the basis of First Amendment activities.[59]

In order to thwart future attacks, law enforcement must have the legal ability to gather information on suspected terrorists. In this regard, the Bush administration is preparing for a sequel to the Patriot Act, since many of the provisions will expire in December 2005, unless renewed.

## V. CONCLUSION

America's technological advances in cyber technology are unmatched. As often is the case, however, a country's greatest strength can also prove to be a critical weakness. America's dependency on the cyber world opens new vulnerabilities to a different type of terrorist attack. A cyber attack can target an actual computer networking system that can cripple a critical infrastructure. It can also manifest itself in a conventional explosive attack on physical structures. Former FBI Director, Louis Freech claimed that "the FBI believes cyber-terrorism, the use of cyber-tool to shut down, degrade, or deny critical national infrastructures, such as energy, transportation, communications, or government services, for the purpose of coercing or intimidating a government or civilian population, is clearly an emerging threat."[60]

[58] *Id.*
[59] *See* Ronald Plesser, "USA Patriot Act for Internet and Communications Companies," *Computer & Internet Lawyer*, march 2002.
[60] *See* Dan Verton, Black Ice: The Invisible Threat of Terrorism, 249, (2003).

A pesar de los esfuerzos para " endemoniarla" la Ley Patriota; las provisiones son actualmente un esfuerzo de buen juicio para detener futuros ataques terroristas, particularmente en el reino del terrorismo-cibernético. Comentando sobre el número de gobiernos locales que han pasado las resoluciones o las leyes en contra de la Ley Patriota, un comentador del Departamento de Justicia anotó que muchos de los decretos estaban basados en información "errónea" sobre le ley y que la Ley Patriota " ha sido una de las más importantes herramientas que el Congreso haya dado al gobierno para luchar contra el terrorismo y así prevenir ataques terroristas[58]. De hecho, muchas provisiones en la Ley Patriota hablan a los artículos de procesos de interés vencidos . Por ejemplo, la enmienda 214 de la Ley Patriota declara que una orden judicial no debe autorizar la recolección de información de inteligencia extranjera para una investigación concerniente a una persona norteamericana o de vigilancia cuando una persona ha sido singularizada solamente según actividades de primera enmienda[59].

Para frustrar futuros ataques, la ejecución de la ley debe tener la habilidad legal para reunir información sobre supuestos terroristas. La administración Bush, en esta consideración, está preparando una secuela de la ley Patriota, desde que muchas de las provisiones expirarán en diciembre del 2005, a no ser que se renueven.

## V. CONCLUSIÓN

Los avances tecnológicos americanos en cuanto a tecnología cibernética son incomparables. Tan a menudo, es el caso, sin embargo, la fuerza más grande de un país también puede demostrar ser una debilidad crítica. La dependencia americana en el mundo cibernético abre nuevas vulnerabilidades a diferentes clases de ataques terroristas. Un ataque cibernético puede apuntar al sistema de red de computadores que puede lisiar una infraestructura crítica. También puede manifestarse esta misma en un ataque explosivo convencional contra estructuras físicas. El actual Director del FBI, Louis Freech reclama que "el FBI cree que el terrorismo cibernético, el uso de herramientas cibernéticas para apagar, degradar o negar los servicios del gobierno, para el propósito de obligar o intimidar a un gobierno o a una población civil, es claramente una amenaza emergente"[60].

[58] *Id.*
[59] *Ver* Ronald Plesser, "USA Patriot Act for Internet and Communications Companies," *Computer & Internet Lawyer*, marzo 2002.
[60] *Ver* Dan Verton, Black Ice: The Invisible Threat of Terrorism, 249, (2003).

It is a threat that must be met with the same recognition and gravity as a physical terrorist attack. In order to secure the nation against cyber terrorism security officials must not be lured into believing that terrorist organizations, such as Al-Qa'eda, lack the necessary equipment and knowledge needed to implement such an attack. Top Al-Qa'eda officials have already expressed their intent to attack the U.S. economy and infrastructures by using the Internet.

The United States must heed these warnings. A valuable tool in this effort is the Patriot Act coupled with the general framework set out by the National Strategy to Secure Cyberspace. Unfortunately, the complacent habit of dealing with known threats has not imparted a sense of urgency that will ultimately be necessary to protect the cyber world. The provisions outlined above must be strengthened in the coming years so that the cyber world is as safe of a place to exist as the physical world.

Es una amenaza que debe ser enfrentada con el mismo reconocimiento y gravedad que un ataque terrorista físico. Para asegurar la nación contra el terrorismo cibernético los oficiales de seguridad no deben de ser atraídos a creer que las organizaciones terroristas, tales como Al-Qa'eda, no poseen el equipo necesario y el conocimiento necesario para implementar un ataque de tal magnitud. Los oficiales de mayor rango de Al-Qa'eda ya han expresado su intención de atacar la economía de los Estados Unidos y las infraestructuras utilizando Internet.

Los Estados Unidos deben considerar estos avisos. Una herramienta valiosa en este esfuerzo es la Ley Patriota acoplada con un marco general lanzado por la estrategia nacional para asegurar el ciberespacio. Desafortunadamente, el hábito complaciente de negociar con amenazas conocidas no ha impartido un sentido de urgencia que últimamente será necesario para proteger el mundo cibernético. Las provisiones delineadas arriba deben ser reforzadas en los años venideros para que el mundo cibernético sea tan seguro, como un lugar para existir como el mundo físico.