

IN FEAR OF CYBERTERRORISM: AN ANALYSIS OF THE CONGRESSIONAL RESPONSE

Tara Mythri Raghavan*

I. INTRODUCTION

The 9/11 attacks on the World Trade Center and Pentagon not only left the United States a nation in mourning, but they also left the government wondering what insidious acts would follow.¹ In its attempt to discover all the possible ways terrorists could strike, the government inadvertently stumbled onto a problem that has plagued this nation for many years: weaknesses in our national security system. While evaluating national security risks, government bodies soon realized that our country's weakest links could be found in the computer networks that run the national infrastructure's critical systems.² This realization has led to the government's new focus on combating cyberterrorism.

Unfortunately, cyberterrorism remains a viable option for any individual or group wanting to use it to further their goals. While bombing physical targets may attract unwanted attention and raise the risk of failure,³ cyberterrorist attacks can be orchestrated more accurately and easily,⁴ and due to the remote location of the preliminary step, the perpetrators are less detectable.⁵ Additionally, cyberterrorism is a much more pressing concern for American citizens than physical threats largely because computers lie at the very heart of American infrastructure and perform critical functions, ranging from storing vital information to controlling power delivery, communications, aviation, and financial services.⁶ It is hardly surprising then that the government

* J.D. University of Illinois College of Law, 2003.

1. Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1, 2-3 (2002).

2. See Mark G. Milone, *Hackivism: Securing the National Infrastructure*, 58 BUS. LAW. 383 (2002). A successful attack on our critical computer networks might initiate "major disruptions that could unravel our economy, diminish our quality of life, and generally destabilize the nation." *Id.* at 384.

3. Brenner & Goodman, *supra* note 2, at 11.

4. See *id.* at 14.

5. *Id.* at 25.

6. Peter Lichtenbaum & Melanie Schneck, *The Response to Cyberattacks: Balancing Security and Cost*, 36 INT'L LAW 39 (2002).

recently has stepped up its efforts to promote computer and network security so as to prevent cyberterrorist attacks.

In its quest to improve cybersecurity, Congress has enacted several forms of legislation over the past two years. The controversial Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”),⁷ was crafted and enacted just six weeks after the 9/11 attacks.⁸ The subsequent Cyber Security Enhancement Act of 2002 (“CSEA”),⁹ which was signed into law as part of the Homeland Security package, also improves upon the Computer Fraud and Abuse Act of 1986 (“CFAA”) ¹⁰ by requiring stiffer penalties for computer crimes than were previously imposed.¹¹ On November 27, 2002, President George W. Bush signed the Cyber Security Research and Development Act (“CSRDA”),¹² which promotes research and development in the relatively unexplored and under-funded area of cybersecurity.¹³ In 2003, several other bills were introduced that also address cybersecurity issues.¹⁴

This essay provides insight into the recent cybersecurity-related laws passed by Congress. Part II provides a synopsis of past private and government actions, revealing that computer security was actually a concern long before 9/11. Despite the government’s prior awareness of cybersecurity concerns, 9/11 became the catalyst that further accelerated congressional action. In Part III, an analysis of the pertinent language and legislative history of the above-mentioned statutes, along with a review of some current bills before Congress, shows that the government is both conscientious and serious about national security in the world of computers. The laws will have far-reaching implications on U.S. citizens, foreigners, and the world as a whole. In Part IV, some of these implications are examined.

7. Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in 8 U.S.C. §§ 1226a, 1379; 15 U.S.C. § 1681v; 18 U.S.C. §§ 175b, 1993, 2339, 2712; 22 U.S.C. §§ 262p-4r, 7210, 7211; 31 U.S.C. §§ 310, 311, 5318A, 5319; 42 U.S.C. §§ 3714, 3796c-1, 5195c; 49 U.S.C. § 5103a; and 50 U.S.C. §§ 403-5b to 403-5d, 1861, 1862) [hereinafter USA PATRIOT Act].

8. 18 U.S.C. § 1 (2001 & Supp. 2003). President Bush signed the USA PATRIOT Act into law on October 26, 2001. Milone, *supra* note 2, at 389. The law protects the national infrastructure by easing the restrictions placed on electronic surveillance and by amending provisions of the Consumer Fraud and Abuse Act to increase penalties for cybercrimes. *Id.*

9. Pub. L. No. 107-296, 116 Stat. 2156 (codified as amended in 6 U.S.C. § 145 (2002 & Supp. 2003)) [hereinafter CSEA].

10. Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended in 18 U.S.C. § 1030 (2002 & Supp. 2003)) [hereinafter CFAA]. The initial substance of the CFAA was originally enacted in 1984, but amendments in 1986 drastically altered the law. Prior to being amended by the USA PATRIOT Act in 2001 and the CSEA in 2002, the substance had also been amended in small part in 1988, 1989, 1990, and 1994, and extensively in 1996. 18 U.S.C. § 1030 (Supp. 2003).

11. 6 U.S.C. § 145 (2002 & Supp. 2003).

12. Pub. L. No. 107-305, 116 Stat. 2368 (codified as amended in 15 U.S.C. §§ 7401–7409 (Supp. 2003)) [hereinafter CSRDA].

13. 15 U.S.C. §§ 7401–7409 (2002 & Supp. 2003).

14. *See, e.g.*, National Cyber Security Leadership Act of 2003, S. 187, 108th Cong. (2003); Justice Enhancement and Domestic Security Act of 2003, S. 22, 108th Cong. (2003).

II. SETTING THE BACKDROP FOR THE LEGISLATION

A. Before September 11, 2001

Even before 9/11, computer security was a particularly serious concern for U.S.-based companies. *Computerworld* published a report detailing an October 2000 computer attack on the Microsoft Corporation, in which hackers disguised themselves as offshore workers of the company in order to gain access to Microsoft's internal network.¹⁵ The Center for Strategic and International Studies subsequently recognized that if Microsoft could be targeted, no company was safe.¹⁶ Worried companies have continued to install firewalls and anti-virus software, resulting from concern that such weaknesses in their computer networks were vulnerable to criminal hacking.¹⁷ Their fears have not proven to be unreasonable: tech-savvy criminals have found numerous ways to make mischief in the computer world over the years.

One way that unauthorized users have intruded upon computer systems is by accessing ports, which allow entry into networks.¹⁸ Using this method, these "hackers" have gleaned important business and other data, which they have then attempted to use for their own agenda.¹⁹ In 1999, the government detected 22,144 attacks against Department of Defense computers.²⁰ Programmers have also distributed malicious codes, commonly known as "malware," in order to disrupt computer networks.²¹ By designing a computer virus, a Trojan horse, or a worm,²²

15. Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense*, 38 STAN. J. INT'L L. 207, 209 (2002) (citing Dan Verton, *Think Tank Warns that Microsoft Hack Could Pose National Security Risk*, COMPUTERWORLD, at <http://www.computerworld.com/securitytopics/security/story/0,10801,55656,00.html> (Dec. 27, 2000)).

16. *Id.* (citing ARNAUD DE BORCHGRAVE ET AL., CTR. FOR STRATEGIC & INT'L STUDIES, CYBER THREATS AND INFORMATION SECURITY: MEETING THE 21ST CENTURY CHALLENGE iv (2000), available at <http://www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf>).

17. See Milone, *supra* note 2, at 388. See generally, *Technology Briefing: Security Best Practice; Know Your Enemy*, COMPUTING, Dec. 3, 1998, at 52 (advising companies to set up firewalls to protect themselves).

18. Milone, *supra* note 2, at 387. The unauthorized intruder can enter systems rather easily by finding holes in the operating systems or by guessing the password to enter. *Id.*

19. See, e.g., *United States v. Riggs*, 739 F.Supp. 414, 416-17 (N.D. Ill. 1990). The defendants, Riggs and Neidorf, gained unauthorized access into Bell South's computer system and downloaded an enhanced 911 (E911) computer text file, which Bell South considered proprietary. The defendant was charged under the federal wire fraud act, 18 U.S.C. § 2314. *Id.*

20. Jensen, *supra* note 15, at 210 (citing Jim Wolf, *Hacking of Pentagon Computers Persists*, WASH. POST, Aug. 9, 2000, at 23).

21. Milone, *supra* note 2, at 387. See generally *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991) (affirming conviction of defendant who was convicted of violating the CFAA for his transmission of a computer "worm" into a group of national networks that were connecting university, governmental, and military computers).

22. A virus is a program or piece of code that runs on an individual computer without the user's knowledge, and which can continue to replicate and spread whenever an infected file is run until a system is overloaded and shuts down. A Trojan horse is a program that masks a malicious attack inside a downloadable useful function, and which depends on the user installing it each time. A worm is similar to a virus but is self-replicating and can contaminate an entire network system. See Kirk

these programmers have been able to inflict massive confusion and economic loss. The “I Love You” computer worm, for example, caused more than \$11 billion in losses in 2000.²³ Computer deviants have also utilized denial of service attacks, which force a targeted system to shut down, preventing legitimate users from entering.²⁴ The need for adequate means to combat such problems has been a government concern for a long time.

1. Legislative Means Used to Combat Cybercrimes Prior to 9/11

Traditionally, the government has relied on its federal criminal laws to protect against cyberthreats.²⁵ Prior to the enactment of the CFAA, the federal wiretapping statute was the only law that held people responsible for electronic crimes.²⁶ Unfortunately, the wiretapping statute insufficiently addressed computer concerns. For example, while email was considered to be “wire communication” under the statute,²⁷ courts interpreted the law to require acquisition of any wire communication while it was being sent. In the case of email, however, this is often not possible, and consequently, the federal wiretapping statute provided insufficient remedies for such fraud.²⁸ It was only when the CFAA was first enacted in 1984 that a federal statute expressly addressed computer crimes.

The CFAA makes it unlawful for an unauthorized person to access a protected computer in order to obtain information, acquire something of value through fraudulent means, or damage the computer of another.²⁹ The CFAA also prohibits the dissemination of malware, which can intentionally damage a protected computer.³⁰ Moreover, persons who suffer damage due to violations of the statute are allowed to sue for compensatory damages.³¹ Such damages include “any impairment to the integrity or availability of data, a program, a system, or information,”³² and those that cause losses aggregating at least \$5,000 in value during any

Hausman et al., *Identifying Nonessential Services and Attacks*, InformIT, at http://www.informit.com/isapi/product_id~%7BADDCDB2C-D91A-491F-82B4623B26F2507A%7D/element_id~%7BFE70EBE9-A9AD-4AF4-91EC-64090660DB21%7D/st~%7B20492063-6F3F-4FB5-A2CE-DC4AF32E0E8C%7D/content/articlex.asp (July 4, 2003).

23. Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1004 (2001).

24. Milone, *supra* note 2, at 388. The denial of service attacks on Yahoo!, eBay, E*Trade, and other sites apparently caused \$1.2 billion in damages. Katyal, *supra* note 23, at 1004.

25. See Lichtenbaum & Schneck, *supra* note 6, at 40. See also Riggs, 739 F. Supp. at 414; *Morris*, 928 F.2d at 504.

26. 18 U.S.C. § 2510 (2000).

27. *Id.* § 2510(1).

28. See generally *United States v. Turk*, 526 F.2d 654 (5th Cir. 1976).

29. 18 U.S.C. § 1030(a)(5)(B).

30. *Id.* § 1030(a)(5)(A).

31. *Id.* § 1030(g).

32. *Id.* § 1030(e)(8).

one-year period to one or more individuals.³³ The punishment for any violation of the CFAA is a fine and/or imprisonment, where the prison term is limited to: (1) not more than one year for the first conviction; (2) five years if the offense was committed for the purposes of commercial advantage or private financial gain, in furtherance of any criminal or tortious act, or if the value of the information obtained exceeds \$5,000; and (3) ten years for the second conviction.³⁴

Since 1986, the CFAA has been amended several times. A 1994 amendment prohibited unauthorized, intentional access to federal computers.³⁵ Most recently, the USA PATRIOT Act and the CSEA have amended the CFAA to address cyberattacks and enhance the penalties for such attacks.³⁶

Courts have also utilized the Electronic Communications Privacy Act of 1986 (“ECPA”),³⁷ the Economic Espionage Act of 1996 (“EEA”),³⁸ and various state criminal statutes³⁹ in order to prevent the disruption of computer networks.⁴⁰ The EEA imposes civil and criminal liability for taking control of another person’s trade secrets, including doing so through computer intrusion. While the EEA does not specifically refer to “computer hacking,” the language of the act is sufficiently broad so as to encompass such intrusions. The problem with the EEA, however, has been that private citizens and corporations do not have standing to sue, leaving only the government to pursue enforcement.⁴¹

Liability can also rise from the ECPA when a computer intrusion is targeted towards obtaining, altering, or preventing access to a stored electronic communication, such as e-mail.⁴² The ECPA amended Title

33. *Id.* § 1030(a)(5)(B)(i). In *United States v. Middleton*, 231 F.3d 1207, 1210 (9th Cir. 2000), the Ninth Circuit Court of Appeals held that Congress clearly intended to include corporations in its definition of “one or more individuals.”

34. *Id.* § 1030(c).

35. *Id.* § 1030(e)(2) (1994). That amendment defined a “federal interest computer” to be one that is:

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution’s operation or the Government’s operation of such computer; or (B) which is one of two or more computers used in committing the offense, not all of which are located in the same State.

Id.

36. *See infra* Part III.A.

37. Pub. L. No. 99-508, 100 Stat. 1848 (codified in various sections of 18 U.S.C. (2003)) [hereinafter ECPA].

38. Pub. L. No. 104-294, 110 Stat. 3488 (codified in 18 U.S.C. § 1831 (2003)) [hereinafter EEA].

39. There have been very few actual prosecutions under state law. In one of those few cases, for example, the Arizona Court of Appeals held that the defendant did not damage his employer’s program by encoding it because he did so with the permission of his employer under Arizona law. *State v. Moran*, 784 P.2d 730, 730–31 (Ariz. Ct. App. 1989).

40. Lichtenbaum & Schneck, *supra* note 6, at 40.

41. *See* 18 U.S.C. § 1836.

42. *See* Milone, *supra* note 2, at 399.

III of the U.S. Code in response to changes in communication technology.⁴³ Violations of § 2511 may result in a fine and/or imprisonment of not more than five years.⁴⁴

State criminal statutes also provide a means for the government to combat cyberattacks. Arizona and Florida enacted the first computer crime statutes in 1978.⁴⁵ Vermont was the last state to enact a computer crime law, which it did in 1999.⁴⁶ In Illinois, the Computer Crime Prevention Law⁴⁷ imposes criminal liability on a person engaging in computer tampering or computer fraud.⁴⁸ The Illinois Electronic Mail Act⁴⁹ goes a step further and provides for civil liability against persons sending unsolicited and spam e-mail.⁵⁰ While these acts have provided the government with a few tools to enhance cybersecurity, they have insufficiently dealt with the multiple problems that have arisen since 9/11.

2. Non-Legislative Efforts

The federal government has also engaged in several non-legislative efforts to address computer security concerns. More than a decade ago, the National Research Council addressed the problem, warning specifically of potential deliberate cyberterrorist attacks in its report, *Computers at Risk*.⁵¹ In 1997, President Clinton's Commission on Critical Infrastructure Protection issued a report that subsequently led to the issuing of Presidential Decision Directive 63 ("PDD 63").⁵² PDD 63 prompted federal agencies to develop critical infrastructure protection plans and encouraged a strategy to protect the nation from cyberattacks.⁵³ While the federal government has previously taken a few actions to address individual cybercrimes, comprehensive cybersecurity has only become a primary governmental focus after 9/11.

B. After 9/11

Following 9/11, the interest in computer security skyrocketed, despite the fact that America's computer-dependent infrastructure was

43. *Id.*

44. 18 U.S.C. § 2511(4)(a) (Supp. 2003).

45. Julie A. Tower, *Hacking Vermont's Computer Crimes Statute*, 25 VT. L. REV. 945, 954 (2001). Arizona and Florida began the long trek towards updating the criminal statutes to the computer age in 1978, and other states followed suit over the course of the next few decades. *Id.* at 954–55.

46. *Id.*

47. 720 ILL. COMP. STAT. 5/16D (2003).

48. *Id.*

49. 815 ILL. COMP. STAT. 511/10 (Supp. 2003).

50. *Id.*

51. Lichtenbaum & Schneck, *supra* note 6, at 39.

52. *Id.* at 41.

53. *Id.*

not even specifically targeted in the terrorist attacks.⁵⁴ In fact, the Internet has been fairly unscathed by international terrorism.⁵⁵ Perhaps it was the increase in regular cyberattacks after 9/11 that propelled the government into action. According to the Computer Emergency Response Team (“CERT”), the attacks on computers increased nearly 160 percent in 2001 alone.⁵⁶ There was a nearly six-fold increase in the number of vulnerability reports received by the CERT in 2001 compared to those received in 1999.⁵⁷ Recent attacks on Microsoft systems have suggested the government’s post-9/11 urgency regarding cybersecurity is warranted.⁵⁸

Since 9/11, governmental agencies have grown more introspective about their lack of computer security, disclosing their security concerns more readily than ever before.⁵⁹ The Justice Department has proposed classifying several cybercrimes under the CFAA as acts of terrorism.⁶⁰ Attorney General John Ashcroft argued that the proposal’s definition of terrorism was not overly broad, even though it was broad enough “to include things like assaults on computers, and assaults designed to change the purpose of government.”⁶¹ The events of 9/11 prompted President Bush to address the computer security concerns facing the nation, his actions included naming Richard Clarke as the President’s Special Adviser for Cybersecurity and creating the Office of Homeland Security.⁶²

Companies such as Microsoft are also now giving security issues higher priority.⁶³ Even universities, after some government prodding, have taken precautions to prevent cyberattacks against their vulnerable computer systems.⁶⁴ In general, “[c]ybersecurity and the protection of

54. *Id.*

55. *Id.*

56. Byron Acohido, *Agency Raises the Bar on Tech Security*, USA TODAY, Feb. 27, 2002, at 7B, available at <http://www.usatoday.com/tech/news/2002/02/27/security.htm>.

57. H.R. REP. NO. 107-355, at 3 (2002).

58. See, e.g., Tim Lemke, *Computer Worm Not Fully on Hook Yet; S. Korea Among Some Still Worried*, WASH. TIMES, Jan. 27, 2003, at A01.

59. See, e.g., *Computer Security: How is the Government Doing? Oversight Hearing Before the House Subcomm. on Gov’t Efficiency, Fin. Mgmt., and Intergovernmental Relations*, 107th Cong. (2001) (opening statement of Steve Horn, Chairman, House Subcomm. on Gov’t Efficiency, Fin. Mgmt. and Intergovernmental Relations), available at http://www.house.gov/reform/gefmir/hearings/2001hearings/1109_computer_security/1109_witnesses.htm. A full two-thirds of federal agencies, including the crucial Departments of Defense, Energy, Transportation, and Health and Human Services, received failing grades in regards to computer security). *Id.*

60. Kevin Poulsen, *Hackers Face Life Imprisonment Under “Anti-Terrorism” Act*, SecurityFocus, at <http://online.securityfocus.com/news/257> (Sept. 24, 2001). Under the Department of Justice’s proposal, Web site defacers and hackers would be considered guilty of terrorist actions. *Id.*

61. *Id.*

62. Lichtenbaum & Schneck, *supra* note 6, at 43.

63. See Acohido, *supra* note 56. Bill Gates declared security the number one priority for Microsoft, ordering over 8,000 programmers to spend a month to work on the matter. *Id.*

64. See *id.* After the Center for Internet Security’s software found several vulnerabilities in Virginia Tech’s network of 24,000 computers, the Center gave the university a program to plug the security holes. *Id.*

critical computer infrastructure have become a hot topic at trade shows, with vendors...and products springing up almost weekly.”⁶⁵ While private citizens and businesses have become much more aware of security concerns since 9/11, until recent legislation was enacted in the area, the government remained unable to combat any cyberterrorist scares. This new legislation provides a method for the government to explore cyberterrorist problems, and conceivably, to find solutions to them.

III. THE LEGISLATION

A. *The USA PATRIOT ACT*

1. *Legislative History*

The USA PATRIOT Act was enacted in response to the events of September 11, 2001. Those events prompted President Bush to declare a state of emergency on September 14, 2001.⁶⁶ The House of Representatives addressed the crisis by introducing the PATRIOT Act of 2001 less than one month later on October 2.⁶⁷ The Senate followed suit two days later with the introduction of the USA Act of 2001.⁶⁸ Once both the Senate and House bills had passed their respective chambers they were incorporated under H.R. 3162, the USA PATRIOT Act, and reintroduced to both chambers.⁶⁹ On October 24, 2001, the Act was approved by a vote of 357 to 66 with “few hearings and little debate” in the House, and it passed the Senate the next day by an overwhelming vote of 96 to 1.⁷⁰ The main controversy in the House was that the Democrats only received two copies of the bill prior to the vote and did not have time to familiarize themselves with its implications.⁷¹ Senator Russell Feingold, the sole dissenter in the Senate, felt that the representatives made their decision in haste without even reading the

65. Sam Costello, *Sept. 11-driven Security Concerns to Drive RSA Show*, InfoWorld, at <http://archive.infoworld.com/articles/hn/xml/02/02/14/020214hnrsshshow.xml> (Feb. 14, 2002).

66. John W. Whitehead & Steven H. Aden, *Forfeiting “Enduring Freedom” for “Homeland Security”: A Constitutional Analysis of the USA PATRIOT Act and the Justice Department’s Anti-Terrorism Initiatives*, 51 AM. U. L. REV. 1081, 1086 (2002).

67. H.R. 2975, 107th Cong. (2001). The House version passed on October 12, 2001. *Id.*

68. S. 1510, 107th Cong. (2001). The Senate version passed on October 11, 2001. *Id.*

69. The new USA PATRIOT Act was introduced in Congress on October 23, 2001, by Representative F. James Sensenbrenner, Jr. H.R. 3162, 107th Cong. (2001).

70. Steven A. Osher, *Privacy, Computers and the PATRIOT Act: The Fourth Amendment Isn’t Dead, But No One Will Insure It*, 54 FLA. L. REV. 521, 522–23 (2002) (quoting Laura Donohue & Jim Walsh, *PATRIOT Act—A Remedy for an Unidentified Problem*, S.F. CHRON., Oct. 30, 2001, at A17, available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/10/30/ED10681.DTL>).

71. *Id.* at 522.

summaries, let alone the actual bill.⁷² The President signed the Act into law on October 26, 2001.⁷³

2. Key Provisions

While the USA PATRIOT Act addresses several issues, only certain key provisions relate to cybersecurity and other computer concerns. Primarily, the Act revamped certain portions of federal law, easing the restrictions on electronic surveillance to facilitate the capture of terrorists. Federal wiretapping statutes previously prohibited electronic eavesdropping using computers and other electronic communications.⁷⁴ These limitations, however, also prevented authorities from intercepting communications to and from a computer system trespasser. The USA PATRIOT Act enables such computer surveillance.⁷⁵ The Act also contains anti-money laundering provisions in order to deny terrorists the opportunity to gain financially from their actions.⁷⁶ While Title III of the U.S. Code previously excluded terrorism and computer crimes from the predicate offense list, the USA PATRIOT Act now includes such crimes.⁷⁷

The majority of the cybersecurity provisions found in the USA PATRIOT Act are amendments to the CFAA.⁷⁸ For example, the Act amends the CFAA to increase the maximum penalty for hacking from ten to twenty years.⁷⁹ It also extends the CFAA's definition of a "protected computer" to include computers located outside the United States.⁸⁰ Finally, the USA PATRIOT Act expands the definition of loss under the CFAA to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition

72. *Id.* at 523 (citing Robert Scheer, *With Powers Like These, Can Repression Be Far Behind?*, L.A. TIMES, Oct. 30, 2001, at <http://www.latimes.com/news/opinion/la-oe-scheer30oct30.story>).

73. President Bush raised the technology issues addressed in the USA PATRIOT Act at the signing:

Surveillance of communications is another essential tool to pursue and stop terrorists. The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones.

As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology. Investigations are often slowed by limits on the reach of federal search warrants. Law enforcement agencies have to get a new warrant for each new district they investigate, even when they're after the same suspect.

President George W. Bush, Address at the White House Signing of the USA PATRIOT Act of 2001 (Oct. 26, 2001), available at http://www.pbs.org/newshour/bb/terrorism/bush_terrorismbill.html.

74. 18 U.S.C. § 2511 (1994).

75. USA PATRIOT Act § 217 (codified as 18 U.S.C. § 2511(2)(i)(IV)).

76. *Id.* §§ 301–77 (codified as 31 U.S.C. § 5318).

77. *Id.* § 814 (codified as amended at 18 U.S.C. § 1030).

78. Lichtenbaum & Schneck, *supra* note 6, at 42.

79. USA PATRIOT Act § 814(c) (codified as amended at 18 U.S.C. § 1030(c)(4)(C)).

80. *Id.* § 814(d)(1) (codified as amended at 18 U.S.C. § 1030(e)(2)(B)).

prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.”⁸¹

B. The Cyber Security Enhancement Act as Incorporated into the Homeland Security Act

The seeds of the CSEA were planted before 9/11. On May 24, 2001, state and local officials addressed cybercrimes before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee.⁸² Each witness to testify described a need for “better resources, training, standards, and equipment.”⁸³ On June 12, 2001, representatives from three federal agencies agreed before the House Subcommittee that the federal laws regarding the processes and procedures for investigating and prosecuting cybercrimes were outdated.⁸⁴ On June 14, 2001, representatives from the business community also testified to their own cybersecurity problems, urging stricter penalties for cybercrimes.⁸⁵ Only after 9/11, however, did Congress find a need to pass legislation addressing the needs of these different groups.

1. Legislative History

To address the security issues revealed in Congressional hearings, the Public Safety and Cyber Security Enhancement Act of 2002⁸⁶ was introduced on September 20, 2001.⁸⁷ While most of the concerns identified in the Act were addressed by Congress in its implementation of the USA PATRIOT Act, a few problems remained. To solve those remaining problems, Texas Congressman Lamar Smith introduced H.R. 3482, the Cyber Security Enhancement Act of 2002,⁸⁸ in the House of Representatives. There was a hearing with regard to H.R. 3482 before the House Judiciary Committee’s Subcommittee on Crime on February 12, 2002.⁸⁹ H.R. 3482 passed overwhelmingly in the House on July 15, 2002.⁹⁰ The Homeland Security Act of 2002 (“HSA”),⁹¹ which was introduced to the House as H.R. 5005,⁹² incorporated a majority of H.R.

81. *Id.* § 814(d)(5) (codified as amended at 18 U.S.C. § 1030(e)(11)).

82. H.R. REP. NO. 107-497, at 7 (2002). The report was submitted by Rep. Sensenbrenner from the Committee on the Judiciary with regard to the Cyber Security Enhancement Act of 2002. *Id.* at 1.

83. *Id.* at 7.

84. *Id.*

85. *Id.*

86. H.R. 2915, 107th Cong. (2001).

87. *Id.*

88. H.R. 3482, 107th Cong. (2002) (enacted).

89. H.R. REP. NO. 107-497, at 8 (2002).

90. Richard Raysman & Peter Brown, *Homeland Security Means Cyber Security*, N.Y. L.J., Dec. 10, 2002, at 3, available at http://www.brownraysman.com/pubs/articles/pdf/NYLJ_12-10-02.pdf.

91. Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified in 6 U.S.C. § 101-557 (2002)) [hereinafter HSA].

92. H.R. 5005, 107th Cong. (2002) (enacted).

3482 as the CSEA.⁹³ Although the cybersecurity aspects were only added later to H.R. 5005, the bill quickly met the approval of Congress and was signed into law on November 25 of that same year.⁹⁴

2. Key Provisions

Section 225 of the HSA, which contains the provisions of the CSEA,⁹⁵ amends the criminal penalties under the CFAA to address the growing cyberterrorism concerns.⁹⁶ The CSEA increases the maximum penalty for “knowingly or recklessly caus[ing] or attempt[ing] to cause serious bodily injury” to twenty years; for knowingly or recklessly causing or attempting to cause death, the maximum penalty is increased to life in prison.⁹⁷ The CSEA also requests the U.S. Sentencing Commission to consider several factors in determining an appropriate sentence, recognizing the increasingly serious nature and growing number of cybercrimes.⁹⁸ The CSEA widens the exemption from liability under the Stored Communications Act⁹⁹ to encompass service providers who voluntarily provide subscriber information to government authorities.¹⁰⁰

C. The Cyber Security Research and Development Act

In July 2001, the House Science Committee’s Subcommittee on Research held a hearing with regard to the federal interest in promoting information technology research.¹⁰¹ In the hearing, witnesses generally had agreed that there was a lack of focus on computer and network security considering the increased dependence of Americans on information technology.¹⁰² The House Science Committee also recognized that 9/11 had served as a cruel spotlight of sorts, focusing on the nation’s vulnerability to attack.¹⁰³ On October 10, 2001, a month after the 9/11 attacks, the House Science Committee had reconvened to determine the vulnerabilities of the computer infrastructure and to further discuss the need for research to alleviate some of the concerns.¹⁰⁴ Both hearings “offered a sobering view of the security of our nation’s critical infrastructures and highlighted the lack of world-class research

93. See HSA § 225 (2002) (codified in 6 U.S.C. § 145 (2002)).

94. See 6 U.S.C. § 101 (2002).

95. See HSA § 225.

96. *Id.* § 225(g) (codified in 18 U.S.C. § 1030(c)).

97. *Id.* § 225(g)(4) (codified in 18 U.S.C. § 1030(c)(5A-5B)).

98. *Id.* § 225(b) (added as a note to 28 U.S.C. § 994 (2002)).

99. The Stored Communications Act was passed as part of the ECPA (codified in 18 U.S.C. §§ 2701–11).

100. *Id.* § 225(d) (codified in 18 U.S.C. § 2702(b)(7)).

101. H.R. REP. NO. 107-355, at 5 (2002).

102. *Id.* at 5–6.

103. See *id.* at 2.

104. *Id.* at 6.

being conducted to address these cyber security needs.”¹⁰⁵ On July 16, 2001, the Senate Subcommittee on Science, Technology, and Space, under the Committee on Commerce, Science, and Transportation, also held a hearing to address cybersecurity, entitled “Holes in the Net: Security Risk and the E-Consumer.”¹⁰⁶

1. Legislative History

In a bipartisan effort, Representatives Boehlert and Hall introduced the CSRDA on December 4, 2001.¹⁰⁷ The bill incorporated several provisions of H.R. 3316, which was introduced by Representative Brian Baird.¹⁰⁸ Testimony at the Science Committee’s hearing on December 12, 2001, indicated that experts from academia, industry, and the government felt that the United States did not place enough focus on computer security.¹⁰⁹ These same individuals felt that few top researchers were interested in the topic, and that something had to be done to encourage those skilled researchers to pursue the field.¹¹⁰ Some individuals were particularly upset that the government did not have any agency to oversee computer security research and development.¹¹¹ Moreover, their disappointment was apparent with regard to private industry input.¹¹² Many felt there were hardly any incentives for private industry to look into computer security.¹¹³

Senator Wyden introduced the Senate’s version of the bill on April 17, 2002.¹¹⁴ An amendment to the bill, as offered by Senators Wyden and Edwards, added provisions from S. 1900 and S. 1901 into the bill on May 17, 2002. This amendment included a provision for a loan forgiveness program for doctoral students agreeing to teach cybersecurity for five years, a provision regarding information security benchmarks, and provisions to enhance ethnic and racial diversity in the National Science Foundation’s cybersecurity programs.¹¹⁵ H.R. 3394 was endorsed by

105. Press Release, House Committee on Science, Committee Approves Bills to Improve Cyber Security, Information Technology Research (Dec. 6, 2001), *available at* <http://www.house.gov/science/press/107pr/107-139.htm>.

106. S. REP. NO. 107-239, at 3 (2002). The Senate held another such hearing on April 24, 2002, entitled “Homeland Security and the Technology Sector.” *Id.*

107. H.R. 3394, 107th Cong. (2002) (enacted as 15 U.S.C. §§ 7401-7409).

108. H.R. REP. NO. 107-355, at 6 (2001).

109. Press Release, Committee on Science, Chairman Boehlert Gives Cyber Security Address at ITAA Forum (Dec. 12, 2001), *available at* <http://www.house.gov/science/press/107pr/107-142.htm>.

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

114. S. 2182, 107th Cong (2002) (enacted as 15 U.S.C. §§ 7401-7409). Senator George Allen and Senator Hillary Rodham Clinton co-sponsored the bill on May 2, 2002. *See* <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:SN02182:@@P> (last visited Dec. 14, 2003).

115. S. REP. NO. 107-239, at 3 (2002).

several organizations as of February 6, 2002.¹¹⁶ The House passed its bill by a vote of 400 to 12 on February 7, 2002.¹¹⁷ On October 16, 2002, Senator Wyden's Amendment, S.A. 4890, was agreed to in the Senate by unanimous consent.¹¹⁸ The House then passed the changed version on November 12, 2002 and the President signed the bill into law on November 27, 2002.¹¹⁹

2. Key Provisions

The CSRDA allows Congress to appropriate nearly \$903 million in federal funds over a period of five years for research and development in the area of computer security.¹²⁰ The National Science Foundation and the National Institute of Standards and Technology will coordinate the use of the funds.¹²¹ Along with earmarking funds for research, the Act also encourages grants to higher education institutions for programs that would increase the number of students interested in studying computer and network security.¹²² One of the controversial aspects of the Act is that it prevents certain foreign individuals from receiving grants simply for being connected to a terrorist supporting state.¹²³

D. Recent Bills in Congress

Since the enactment of the previously named laws, Congress has been busy thinking of other ways to combat cybersecurity concerns. Under the National Cyber Security Leadership Act of 2003, Congress seeks to identify the vulnerabilities in the information technology systems of various agencies.¹²⁴ This Act would provide for funding to the

116. *The Cyber Security Research and Development Act: Letters of Endorsement on H.R. 3394* (Feb. 6, 2002), at <http://www.house.gov/science/cyber/endorse.htm> (last visited Feb. 9, 2003). From the Alliance for Science and Technology Research in America to several universities including Cornell and Syracuse Universities, many research institutions were particularly interested in H.R. 3394. *Id.*

117. Press Release, House Science Committee Democratic Caucus, Computer Security Bill Passes House Overwhelmingly (Feb. 7, 2002), available at http://www.house.gov/science_democrats/releases/02feb07.htm.

118. 148 CONG. REC. S10,601 (2002).

119. Laura Rohde, *President Signs Cybersecurity Bill Into Law*, INFOWORLD.COM, at <http://archive.infoworld.com/articles/hn/xml/02/11/29/021129hnsecurity.xml?s=IDGNS> (Nov. 29, 2002).

120. Brock Read, *House Votes to Authorize Greater Spending on Computer-Security Research*, CHRON. OF HIGHER EDUC. Nov. 29, 2002, at 29 [hereinafter Read, *Computer-Security Research*].

121. 15 U.S.C. § 7409 (2002). Explicit instructions for how this delegating process works fall under preceding sections. *Id.* at §§ 7403–7408.

122. *Id.* at § 7404. Faculty development and training programs are also to be established. *Id.* at § 7404(e).

123. *Id.* at § 7410(b).

No grant or fellowship may be awarded under this Act, directly or indirectly, to any alien from a country that is a state sponsor of international terrorism, as defined under section 1735(b) of Title 8, unless the Secretary of State determines, in consultation with the Attorney General and the heads of other appropriate agencies, that such alien does not pose a threat to the safety or national security of the United States.

Id.

124. S. 187, 108th Cong. § 2 (2003).

Department of Commerce for the National Institute of Standards and Technology to develop guidelines with regard to these vulnerabilities as well as checklists to eliminate them.¹²⁵ Similarly, the Justice Enhancement and Domestic Security Act of 2003 seeks to improve computer security in order to improve border security.¹²⁶ By seeking to identify information technology vulnerabilities of federal agencies and finessing the computer security concerns with regard to border relations, the government is seeking to improve cybersecurity in all arenas.

IV. IMPLICATIONS

A. Negative Implications

1. USA PATRIOT Act and Civil Liberty Issues

The USA PATRIOT Act has already been analyzed for its various problems. The Electronic Frontier Foundation (“EFF”) in particular has had much to say about this Act, criticizing it for its host of problems.¹²⁷ The EFF believes that the expanded surveillance comes without checks and balances.¹²⁸ One of the deepest problems associated with the Act is that the government is allowed to spy on suspected computer trespassers without a court order, infringing on the civil liberties of suspected trespassers.¹²⁹ Furthermore, the law allows Americans to fall under the auspices of the U.S. Foreign Intelligence Agency, which may misappropriate information originally gleaned for the purpose of cybersecurity.¹³⁰ While the protection of cybersystems is a concern, the question becomes whether this security should come at the loss of other freedoms on which the United States prides itself.

2. USA PATRIOT and CSEA: Deterrent or Not?

There is also the question of whether enhanced penalty legislation like the USA PATRIOT Act and CSEA will effectively prevent cyberterrorism. The EFF argues the USA PATRIOT Act is overbroad and fails to focus precisely on the terrorism problem.¹³¹ Clearly the increased penalties under the acts are part of a deterrence mechanism. However, the USA PATRIOT Act does not necessarily provide added

125. *Id.* at § 5.

126. S. 22, 108th Cong. (2003).

127. *EFF Analysis of the Provisions of the USA Patriot Act*, ELECTRONIC FRONTIER FOUND., Oct. 31, 2001, at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html. The EFF worries that the USA PATRIOT Act was hastily conceived. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.*

security, seeking instead to bolster the CFAA penalties.¹³² Stricter punishment may not prevent future cyberterrorist attacks, instead deterring only “teenage hackers.”¹³³ The same may be said for the CSEA, which only focuses on the penalty aspects of cyberattacks by amending provisions of the CFAA rather than concentrating on creating better security measures.

3. *Problems with the Cyber Security Research and Development Act*

While the CSRDA does seek to create increased cybersecurity by funding research and development in the subject matter, the Act is far from flawless. While additional government funding is generally welcome in all research areas, there is always the fear in this particular arena that it may come at the loss of the promotion of the electronic marketplace and communications.¹³⁴ In addition, in an economic slump, one also needs to question where the money to support such research programs will be found.¹³⁵ Congress must target other programs for cuts to provide funds for these new programs. Moreover, an argument can be made that government funds would be better invested in programs more integral to the national infrastructure, including education and defense. There have been no proven cyberterrorist attacks in the United States, and some may argue against spending funds on the unknown.

B. Positive Implications

Amidst the criticism of these laws, there are several possible positive implications stemming from their enactment. The USA PATRIOT Act and CSEA do seek to deter cybercrimes through criminal penalties. While the increased penalties may not prevent anonymous cyberterrorists from striking, they may have the effect of preventing other cybercrimes. Companies have found some benefits from the passage of these laws. Microsoft was particularly pleased with the passage of the CSEA, applauding Congress for granting federal judges more flexibility in imposing sentences for cybercrimes.¹³⁶ The fact that the USA PATRIOT Act allows the government to target suspected computer trespassers may be a quick mechanism to catch the “bad guys.”

132. Lichtenbaum & Schneck, *supra* note 6, at 42.

133. *Id.*

134. *Id.*

135. The real test for the bill was considered to be the appropriation process. Read, *Computer-Security Research*, *supra* note 120, at 29.

136. *Hearing on Cyberterrorism and Critical Infrastructure Before the Subcomm. on Gov't Efficiency, Fin. Mgmt., and Intergovernmental Relations of the House Comm. On Government Reform*, 107th Cong. (July 24, 2002) (prepared testimony of Scott Charney, Chief Security Strategist, Microsoft Corp.), available at <http://www.microsoft.com/presspass/exec/charney/07-24testimony.asp>. Charney stated that sentencing is often dependant on actual economic loss, which is not easily determined in cybercrime cases. *Id.* He consequently applauded the CSEA for delineating other broad relevant issues when deciding sentencing.

The CSRDA promotes corroboration among the information security industry, government, and academic research projects.¹³⁷ There are several areas in which new or additional research is needed.¹³⁸ By funding these neglected areas, the Act bolsters computer security essential to the many businesses relying on information technology.¹³⁹ The CSRDA may in fact fill the loopholes created by the USA PATRIOT Act and CSEA, creating a symbiotic relationship beneficial to all parties involved, except perhaps the cyberterrorists that these acts seek to deter.

V. CONCLUSION

In passing the USA PATRIOT Act, the Cyber Security Enhancement Act, and the CSRDA, Congress sought to prevent cyberterrorism. Based upon years of frustration with regard to cybercrime in general, Congress has set out in recent years to address an issue that affects the national infrastructure's critical systems. While only time will tell whether these different Acts will have their desired effects, there is no denying that the government is serious about tackling the cyberterrorism problem. The recent bills proposed in Congress only serve to highlight that fact.

137. Press Release, Information Technology Association of America, ITAA Applauds Final Passage of Cyber Security R&D Act, (Nov. 12, 2002), *available at* <http://itaa.org/news/pr/PressRelease.cfm?ReleaseID=1037227800> (last visited Feb. 9, 2003).

138. INST. FOR INFO. INFRASTRUCTURE PROTECTION, CYBER SECURITY RESEARCH AND DEV. AGENDA ii (Jan. 2003), *available at* http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf. The Institute for Information Infrastructure Protection, a consortium of twenty-three academic and not-for-profit bodies, suggests that several different areas should be researched, from Wireless Security to Metrics and Models. *Id.* at i-ii.

139. *Homeland Security Legislation Includes Transportation Benefits*, Chemical Market Reporter, Dec. 9, 2002, at 4.