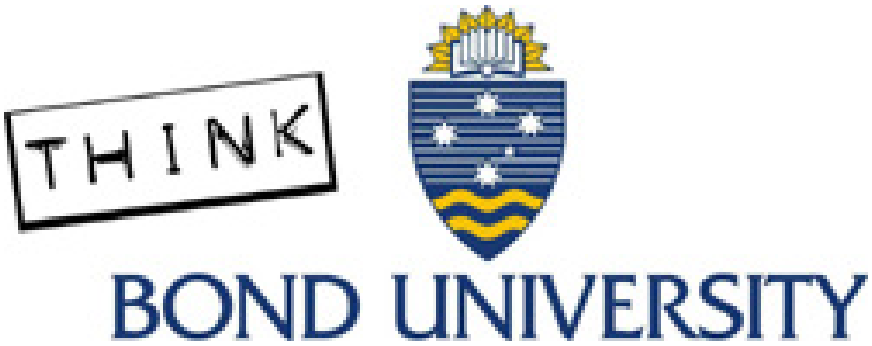

SCHOOL OF BUSINESS

REDUCING COMPUTER INTRUSION IN THE POST PATRIOT ACT ERA

LAWS77-429

ELECTRONIC COMMERCE AND THE LAW

Student ID: **11071217**

Supervisor: **Patrick Quirk**

Enrolled Semester: **September 2000**

Table of Contents

Topic Exploration

This paper examines the topic of computer related crime and how such crime is investigated and prosecuted in the United States. A particular focus is drawn on the "Uniting and Strengthening America by Providing Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001".[1] The passing of this Act into law has enhanced the resources and powers of investigators of computer crime and has escalated the seriousness of offences by classifying certain computer crimes as acts of terrorism. The USA Patriot Act not only augments the power of investigators but creates the provision for the deterrence and prevention of cyberterrorism[2] through a number of means including the expansion of the national electronic crime task force[3]. This report will focus on computer intrusion, and will assess the increased powers provided by the USA Patriot Act, and their effectiveness in reducing the incidence of cyber crime but more particularly computer intrusion.

It can be hypothesised that with widespread adoption of the computer into education, commerce and communication, we as a society are becoming more computer literate and, subsequently, more computer dependant. Individuals and corporations use computer technology to access valuable information be it banking, stock or financial records, customer and employee databases, internal communications or personal files. Corporate establishments such as Amazon[4], Dell[5], E-Bay[6] are among thousands of companies that now rely upon computers and the Internet to provide a global market for trade and commerce. The increased prevalence of computer related trade and commerce, and the growth of the Internet has meant that more and more valuable information must be accessed by computers and computer networks. The increasing prevalence of the Internet was recognised as a potential crime problem by the Clinton Administration issuing Executive Order 13133. This order called for the assembly of a working group to examine how effective America's laws were at prosecution of illegal conduct regarding the Internet, what technologies were required to prosecute unlawful conduct on the Internet and the education of users about unlawful conduct on the Internet.[7]

Increasing access to computer resources including smaller faster and cheaper processors, the growing availability of broadband network connections together with an assumed imbalance in skill level among computer uses and administrators, form a catalyst for increasing computer crime. Computer related crime is a diverse and constantly expanding field, difficult to define. In January of 2000, Janet Reno the then United States Attorney General acknowledged this point proclaiming, "while the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behaviour,".[8] This report examines

---

[1] *USA Patriot Act,* Pub L No 107-56, § 1(a), 115 Stat. 272 (2001).
[2] *USA Patriot Act,* Pub L No 107-56, § 814, 115 Stat. 272 (2001).
[3] *USA Patriot Act,* Pub L No 107-56, § 105, 115 Stat. 272 (2001).
[4] Amazon.com Inc. (NASDAQ: AMZN) http://www.amazon.com
[5] Dell Computer Corporation (NASDAQ: DELL) http://www.dell.com
[6] eBay Inc. (NASDAQ: EBAY) http://www.ebay.com
[7] Clinton William, "Executive Order 13133" (The White House Washington D.C. , August 5 1999) http://resource.lawlinks.com/Content/Legal_Research/Executive_Orders/1999/Technology/executive_order_13133.htm
[8] Reno Janet, "Keynote Address" (National Association of Attorneys General, Stanford Law School California, 10 January 2000) http://www.usdoj.gov/opa/pr/2000/January/007ag.htm

some of this criminal behaviour and reviews a number of the changes the USA Patriot Act delivers in investigating and prosecuting such crimes.

"The Internet …is simply a new medium through which traditional crimes can now be committed".[9] Computer related crime encompasses a diverse range of offences which includes crimes such as: Internet fraud, Intellectual Property theft, child pornography, sale of illegal and controlled substances, securities fraud, online gambling and cyber stalking. Another area that falls under the broad classification of computer crime is computer intrusion, an activity known more popularly as hacking or cracking. Computer intrusion is the area of computer crime that has been chosen as the focus of this paper because of its importance to Electronic Commerce. For the purpose of this paper computer intrusion is defined as *the unauthorised access, or access exceeding current authorisation of a user to an individual computer, or computer system.*

Computer crime and the associated legislation examined within this report are restricted to laws of the United States of America. This is due, in part, to the infancy of legislation relating to computer crimes globally. There is a great deal of debate in reference to matters relating to jurisdiction of cyber crime.[10] The issue of jurisdiction is indeed a significant topic in its self. Given this, cyber jurisdiction is only covered briefly in this paper. As a matter of clarity and consistency the laws examined in this report are that of United States Federal Law. While most of the States have adopted their own independent computer crime laws, the Federal laws are more applicable to the Internet as defined under interstate trade and commerce.

[9] President's Working Group on Unlawful Conduct on the Internet, United States Presidential Authority, *The Electronic Frontier: The Challenge Of Unlawful Conduct Involving the Use of the Internet*, (March 2000), Section I

[10] David Johnson and David Post, 'Law And Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367, IB http://www.cli.org/X0025_LBFIN.html

Unauthorised Access Computer Crime Pre October 2001

26 October 2001 represents the date that President Bush signed into law the USA Patroit Act vastly altering, even if temporarily in some instances, the pursuit and prosecution of computer crime. In the time prior to signing this Act into law, the Pre-Patriot period, a greater majority of computer crime was investigated and prosecuted under the Federal Criminal Code. Some of the more common offences are covered in this section. In relation to computer intrusion the two more pertinent sections are 18 U.S.C: Chapter 47 Sections 1029 and 1030. For the purpose of this report, these sections are covered in detail, while other less relevant sections are briefly reviewed.

18 U.S.C §1029 Fraud and Related Activity in Connection with Access Devices

Subsection (a) 18 U.S.C §1029 states that whoever--

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
(2) knowingly and with intent to defraud traffics in or uses one or more unauthorised access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;
(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorised access devices;
(4) knowingly and with intent to defraud produces, traffics in, has control or custody of, or possess device-making equipment;
(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;
(6) without the authorisation of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—
    (A) offering an access device; or
    (B) selling information regarding or an application to obtain an access device;
(7) and with intent to defraud produces, traffics in, has control or custody of, or possess a telecommunications instrument that has been modified or altered to obtain unauthorised use of telecommunications services;
(8) and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;
(9) uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization;
(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offence affects interstate or foreign commerce, be punished as provided in subsection (c) of [18 U.S.C. §1029 (a)]

Subsection (b) further adds that whoever attempts to commit an offence listed in subsection (a) shall be subject to the same penalties. An attempt is treated as an

offence.[11] Anyone party to a conspiracy of two or more people to commit any of the offences listed in subsection (a), and this offence occurs, they shall be fined up to the maximum penalty, but only imprisoned for up to half the maximum penalty.[12] Subsection (c) specifies the penalties for breaches of subsections (a) and (b). Generally the penalty may include a fine, imprisonment and forfeiture of property, or any combination of these. Prison sentence maximums range from 10-15 years for first offenders and generally 20 years for second offenders. This depends upon which relevant subsection was breached.

This legislation is important to the prosecution of computer intrusion due to the classification of an access device;

> any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);[13]

Thus the definition of an access device can include a password or electronic account number, pin, credit cards, dial in account names or passwords. This definition is also relevant to hackers that use masking units such as IP spoofers, used to obtain access to restricted areas by perceiving to alter the users IP address. Such devices are used to assist in blocking the tracing of unauthorized access. This section is useful to further prosecute individuals after they have breached a system and subsequently use that system to access other networks or computers across telecommunications services such as the Internet.[14] Cases that apply 18 U.S.C. § 1029 will be given after the discussion of Fraud and Related Activity in Connection with Computers[15] as computer hacks often breach both statues.

18 U.S.C §1030 Fraud and Related Activity in Connection with Computers

Statute Summary

The following is a summary of the element of subsection (a)[16]
Subsection (a) Whoever

(1)

- Knowingly accesses a computer without authorisation, or exceeding authorised access
- Obtains information determined by Executive Order or statute to be protected against unauthorised access
- With reason to believe such information could be used to injure The United States or advantage any foreign nation

[11] Fraud and Related Activity in Connection with Access Devices 18 USC § 1029 (b)(1).
[12] Fraud and Related Activity in Connection with Access Devices 18 USC § 1029 (b)(2).
[13] Fraud and Related Activity in Connection with Access Devices 18 USC § 1029 (e)(1) .
[14] Julio Cesar Ardita Case (1996) http://www.chips.navy.mil/archives/96_jul/file3.htm .
[15] 18 USC §1030, (as amended 1996).
[16] 18 USC §1030 (a), (As amended 1996).

- Wilfully communicates, delivers transmits, attempts to, or causes the delivery, communication or transmission to someone not entitled to receive it, or
- Wilfully retains or fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) Intentionally accesses a computer without authorisation or exceeds authorised access, and thereby obtains--
  (A) information in a financial record of a financial institution, credit or consumer agency
  (B) any department of the United States government; or
  (C) any protected computer if the conduct involved an interstate or foreign communication;

(3) Intentionally and without authorization accesses a nonpublic computer of the United States government either for exclusive use of the government or is not but used by the Government and this use is affect by unauthorized access

(4) Knowingly and with intent to defraud, access a protected computer, without or exceeding authorization and by doing so obtains anything of value (beyond the use of the computer) and this value is less than $5,000 in a 1 year period;

(5)
  (A) knowingly causes transmission of a program, information, code, or command resulting in conduct causing damage to a protected computer
  (B) intentionally access protected computer without authorization and recklessly causes damage
  (C) intentionally access protected computer without authorization and causes damage

(6) Knowingly and with intent to defraud traffics any password or similar information used to access a computer without authorization, if
  (A) Such trafficking affects interstate trade or commerce; or
  (B) The computer is used by or for the United States Government

(7) With intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, money or anything of value, transmits in interstate trade or commerce any communication any threat to cause damage to a protected computer

Subsection (b) states that any attempt to commit an offence covered under subsection (a) will be liable for penalties listed in subsection (c).[17] Penalties for such breaches can include a fine and or imprisonment. Violations of (a)(1) may receive a maximum 10 years first offence and 20 years for repeat offenders. Violators of (a)(2), (a)(3), (a)(5)(c) and (a)(6) may receive a maximum 1 year for first offence and 10 years second offence. If, however, the violation of (a)(2) was for commercial advantage or personal gain or for furtherance of criminal or tortious act of law or the value of the information exceeds $5,000 the maximum first offence is increased to 5 years.[18] Violators of (a)(4), (a)(5)(a), (a)(5)(b), and (a)(7), can receive a maximum of 5 years first offence and 10 years second offence.[19]

Subsection (g) makes mention of possible civil action against violators to obtain compensatory damages and injunctive relief, or, other equitable relief for damage or loss due to a violation. The stipulation however is that claims must be lodged within 2 years of the date of complaint or discovery of damage. Damages are limited to

[17] 18 USC §1030 (b), (As amended 1996).
[18] 18 USC §1030 (c)(2)(B) (As amended 1996)
[19] 18 USC §1030 (c), (As amended 1996).

economic damages.[20] Such damage is defined, under this section, as any impairment to the integrity or availability of data, a program, a system, or information that causes losses of at least $5,000, affects or potentially affect medical treatment, diagnosis or care, causes injury or threatens public health or safety.[21]

Other Federal Codes Relating to Unauthorised Computer Crime

18 U.S.C. 1362 Communication Lines, Stations, or Systems

This section addresses wilful and malicious injury or destruction, to works, property or materials that provide a means of communication controlled by United States or used by civil or military defence. In this code an attempt to commit also constitute a violation. If a message is obstructed, hindered or delayed a penalty may be applied. Penalties may include a fine, imprisonment of no longer than 10 years, or both.[22] Such legislation could be applied to a breach of critical infrastructure, or an attack on any network router, switch, hub, cable, microwave, satellite or network equipment. One documented form of Denial of Service (DoS) attack is to disable the primary router which connects a computer to the network. Such an act is designed to make contained computer, or network, inaccessible.[23] This form of DoS attack would constitute a breach of 18 U.S.C. 1362, hence this section is also be relevant to computer intrusion.

18 U.S.C. § 2511 Interception and Disclosure of Wire, Oral, or Electronic Communications

Intentionally intercepting or endeavouring to intercept any wire, oral or electrical communication, or procuring another to do so is a violation of this statute. Use of a device to intercept oral communication is also liable to penalty, as is intentionally disclosing or attempting to disclose contents of communication knowing or with reason to suspect was obtained unlawfully. Disclosing legally obtained communication to obstruct justice also constitutes an offence under this section.[24] There are exceptions to these offences, including court ordered taps and traps, and employees under the normal course of employment.[25] Penalties include fines and or imprisonment of up to 5 years. This section is relevant to computer intrusion as the use of various hacking tools such as packet sniffers, used to seek out information as it travels through the network, are tools commonly used by hackers. Such tools were recognised in the case against a hacker named ‘Smak’.[26] The use of such tools clearly constitutes a breach to this statute.

---

[20] 18 USC §1030 (g), (As amended 1996).
[21] 18 USC §1030 (e)(8)(A-D), (As amended 1996).
[22] 18 USC § 1362
[23] Lasse Huovinen, Jani Hursti, *Denial of Service Attacks: Teardrop and Land*, Department of Computer Science Helsinki University of Technology http://www.hut.fi/~lhuovine/hacker/dos.htmhttp://www.hut.fi/~lhuovine/hacker/dos.htm , at 3 August 2002.
[24] 18 U.S.C. § 2511 (1)(a-e)
[25] 18 U.S.C. § 2511 (2)(a)(i)
[26] Henry Lee, *Hacker Stole Thousands Of Passwords UC Berkeley case shows access flaws,* San Francisco Chronicle, http://www.sfgate.com/cgibin/article.cgi?file=/chronicle/archive/1998/08/13/MN26139.DTL 13 August 1998

18 U.S.C. § 2701 Unlawful Access to Stored Communications

This statute makes it illegal to intentionally exceed authorisation to access a facility through which an electronic communication is stored. Additionally, if during the unauthorised access a stored electronic communication is obtained, altered, or the access prevents an authorised user from obtaining the communication, an offence has been committed. If the intrusion and subsequent offence were of commercial advantage, the penalty includes a fine and or maximum imprisonment of one year for first time offenders, two years for repeat offenders. In other cases a fine and or maximum imprisonment of six months would apply.[27] This section is relevant to computer intrusion as often hackers access email, samba (UNIX method of storage), accounts, after they have gained unauthorised access to the system.

This statute is augmented by 18 U.S.C. § 2703, Disclosure of Contents and 18 U.S.C § 2703, Requirements for Governmental Access. These subsequent sections do not allow service providers or storage, or remote services, to knowingly divulge the content of stored communications unless entitled to it. Such groups entitled include the intended recipient, those to whom the originator has given consent, the operator of the account, and certain government agencies or investigators with court authorisation. Exception is also granted where the operator reasonably believes the information relates to the immediate danger of death or serious physical injury, of instances identified under the Crime Control Act of 1990.[28]

[27] 18 U.S.C. § 2701
[28] Crime control Act of 1990, 42 U.S.C.A. §13032

Alleged Defects of Investigation and Prosecution of Cyber Crime Pre Patriot Act

Director of the National Infrastructure Protection Centre, Michael Vatis, stated in a deposition to a Joint Senate Subcommittee that, "cyber crime presents the most fundamental challenge for law enforcement in the 21st Century".[29] The reasons for this mounting challenge are numerous. Some of these challenges arise from deficiencies in the existing legal framework, while challenges also arise from more ambiguus issues that are difficult to quantify, and furthermore difficult to control. It should be highlighted at this stage that the alleged defects, deficiencies and 'challenge[s]' outlined in this section are applicable prior to the introduction of the USA Patriot Act into law, the pre-Patriot period.

Non Legislative Defects

Increased Incidence of Computer Penetration

One of the most recognised alleged deficiencies in the pre-Patriot era is the inability of investigators to handle the increasing volume of offences and complaints in relation to cyber intrusion. FBI Special Agent Guadalupe confirms this claim stating, "even though the FBI has markedly improved its capabilities to fight cyber intrusions, the problem is growing even faster".[30] Guadalupe further highlights this point stating that in the 1998 financial year the FBI opened 547 computer intrusion cases, this number grew to 1154 in the 1999 financial year[31]. This trend is expected to rise exponentially with the FBI/CSI 2002 Computer Crime and Security Survey finding that of the 503 computer security practitioners surveyed in government, business and education, 90% believed they had detected breaches of computer security in the last 12 months.[32] The reasons for this increase may be attributable to a number of possible explanations.

One reason security experts, including those at Spectrum Systems,[33] cite for the increase is the growing number of computers connected to networks. This is coupled with the rise of information available to computer users necessitated by the increasing number of companies "doing more business on the Internet than ever before"[34]. The wider availability of 'always on' broadband Internet access and the growing speed of these connections are advantageous to system penetrators. Permanent connections and

---

[29] Deposition to Senate Judiciary Committee Criminal Justice Oversight Subcommittee and House Judiciary Committee Crime Subcommittee, Washington D.C., February 29 2000, (Michael A. Vatis) http://www.fbi.gov/congress/congress00/vatis022900.htm

[30] Deposition to a Special Field Hearing Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington D.C., April 21 2000, (Special Agent Guadalupe Gonzalez) http://www.fbi.gov/congress/congress00/gonza042100.htm

[31] Ibid

[32] Computer Security Institute, CSI/*FBI Computer Crime and Security Survey*, (2002) http://www.gocsi.com/press/20020407.html at 10 August 2002

[33] Spectrum Systems, The Why's, What's, Who's and How's of Network Security, (2002), http://www.spectrium-systems.com/wp_security_basics.htm at 11 August 2002

[34] Deposition to a Special Field Hearing Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington D.C., April 21 2000, (Special Agent Guadalupe Gonzalez) http://www.fbi.gov/congress/congress00/gonza042100.htm

high speed are attractive not only in accessing the information, but for the purpose of using these computers as a tool for launching further attacks on other computers. According to Special Agent Gonzalez the skill level required to crack and hack has diminished thanks to downloadable scripts and software tools that have become more sophisticated, yet easier to use. This puts the ability to hack in the hands of the everyday computer users, not just the highly skilled. Such users are also known as 'script kiddies'.[35] The lack of awareness of some staff, management and administrators in various networks may also have contributed to their vulnerability.[36]

Author and journalist Dan Verton suggests that hacking has "become a centrepiece of our popular culture".[37] Increased publicity and mass media attention has made hacking and cracking a "national past time for many curious and rebellious teenagers". The idea that hacking has become an outlet for "civil disobedience", rebellion and activism, is not confined to teenagers. FBI director Louis Freeh acknowledges "hactivism" as a growing credible concern.[38] Evidence of this phenomenon was seen during the conflict in former Yugoslavia where hackers, sympathetic to Serbia, attacked NATO targets including websites and computer systems.[39] Cyber vigilantism also came to the fore when Chinese hackers began to attack United States sites and computers in retaliation for the death of a Chinese fighter pilot when his aircraft collided with an American spy plane in April 2001. American hackers subsequently banded together, under the guise of patriotism, to retaliate by attacking Chinese machines[40]. The Internet has given users a forum to publicise and promote their views and ideals. The added benefit is the increased ability to hide ones identity. This is an attribute, not just favoured by hactivists, but cyber criminals leading to another alleged defect in investigation and prosecution of computer intrusion.

Anonymity of Offenders

The current state of the Internet configuration means that computer users are able to mask or hide their true identity and location. This is due to the fact that the Internet relies upon old standards and protocols that were not initially designed for the uses which are currently being applied. The Internet has grown so large so quickly that the underlying supporting technology is carrying functions well in excess of original specifications and designed functionality. Security was not considered as an essential element of the original Internet Protocol (IP), the backbone of Internet communication. Likewise other communication protocols such as HTTP (web pages), SMTP (email) and FTP (file transfer) were not designed for secure applications. Because of this, users are able to mask their identity or assume the identity of others and utilise these protocols and applications beyond their authorisation. This can be done through the use of specialised tools and software applications like IP spoofers

[35] Ibid.
[36] Spectrum Systems, The Why's, What's, Who's and How's of Network Security, (2002), http://www.spectrium-systems.com/wp_security_basics.htm at 11 August 2002
[37] Dan Verton, *The Hacker Diaries Confessions of Teenage Hackers*, McGraw-Hill (2002) 195.
[38] Deposition to Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary and Related Agencies, Washington D.C., 16 February 2000, (Louis Freeh) http://www.fbi.gov/congress/congress00/cyber021600.htm .
[39] Ibid.
[40] Rebecca Sausner, *"U.S., Chinese Hackers Wage Quiet War"*, Newsfactor Network, (http://www.newsfactor.com/perl/story/9203.html) 24 April 2001.

and used in conjunction with other tools such as multiple relays whereby a hacker may use several different computers simultaneously to intrude upon computer systems. More experienced offenders cover their activity by deleting or altering the system log files. These factors make it difficult to track and obtain a clear audit trail. These issues also create repercussions relating to jurisdiction when tracing the audit trails. Such difficulties will be discussed at a later stage of this report. Security experts[41] and investigators[42] highlight identifying the intruder as one of the key hindrances to prosecuting computer intruders.

Access to Resources

Investigation and prosecution of computer intrusion, indeed the majority of cyber crime, is resource intensive. Resources include manpower, computer power and storage which all equate to substantial financial obligation. Time is also a vital resource when investigating computer crime. Resources also need to be allocated to educate the public as to the existence of laws against computer intrusion. One of the alleged deficiencies of the investigation and prosecution of unlawful activity is the restriction of limited resource allocation. Both the Director of the FBI[43] and the Director of the National Infrastructure Protection[44] stresses the need for continuing and increasing financial support from Congress.

Reluctance to Report Breaches

Reluctance of industry professionals to alert authorities of computer breaches in a timely manner is a critical defect in the investigation and prosecution of computer intrusion. Companies are reluctant to announce breaches to officials as this may be seen as a signal of weakness or incompetency to the market. Such news may affect customer, business partner or investor confidence in the company. In addition, announcing breaches may provoke interest from other potential system attackers.[45] Corporations are also reluctant due to the losses associated with investigation. If a breach occurs it is more likely that critical hardware will have to be analysed which can be costly to replace, or may mean longer downtime. This might further exacerbate the losses associated with the initial breach. The CSI/FBI Computer Crime and Security Survey found that in 2001 34% of those that suffered intrusions reported

---

[41] Dr David Cater, *Computer Crime Categories: How Techno-criminals Operate*, Michigan State University, http://nsi.org/Library/Compsec/crimecon.html .

[42] Deposition to a Special Field Hearing Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington D.C., April 21 2000, (Special Agent Guadalupe Gonzalez) http://www.fbi.gov/congress/congress00/gonza042100.htm

[43] Deposition to Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary and Related Agencies, Washington D.C., 16 February 2000, (Louis Freeh) http://www.fbi.gov/congress/congress00/cyber021600.htm .

[44] Deposition to Senate Judiciary Committee Criminal Justice Oversight Subcommittee and House Judiciary Committee Crime Subcommittee, Washington D.C., February 29 2000, (Michael A. Vatis) http://www.fbi.gov/congress/congress00/vatis022900.htm

[45] Maury Shenk, "Should a Corporation Report a Breach to Law Enforcement?", [volume 1], Secure Business Quarterly, http://www.sbq.com/sbq/digital_forensics/sbq_forensics_reporting_breachs.pdf [pps 4-6]

them to law enforcement. While this figure is rather low, these figures are up from 25% in 2000 and only 16% in 1996.[46]

Legislative Defects

> "The problem of Internet crime has grown at such a rapid pace that the laws have not kept up with the technology." FBI Special Agent Guadalupe Gonzalez[47].

Fast Paced Technology

As illustrated by the point made above by Special Agent Gonzalez, technology, especially the Internet moves very rapidly, however, laws are generally slow in formation and often slower in reformation. Because legislation is frequently written in precise language to remove ambiguity in interpretation, this is at times to the detriment of definitions that evolve with the times. For example statute relating to Pen Registers and Trap and Trace Devices[48] encompass language that is specific to telephone communications. This is because when the statute was drafted in 1986, the knowledge of electronic communications was limited to the technology of the time, and some of this language could be challenged as not relevant to modern electronic communications.[49]

Jurisdictional Issues

While jurisdiction is an ongoing debate in the area of cyber crime, comprehensive coverage of the issues is beyond the scope of this report. The issues covered here are pertinent specifically to the investigation of computer intrusion. The time delay associated with jurisdictional issues can cause significant hindrance to an investigation of computer intrusion. This point has been reiterated continually by experts and investigators including the FBI special agent Peter Trahon[50]. Warrants are issued in Federal courts, but are only exercisable in the district in which they were issued. This means that to trace a communication pertaining to an alleged offence, investigators are often required to seek several court orders in different districts to trace the relevant information. This is further complicated by the fact that a delay in this process can mean the loss of potential investigation time as some providers do not keep detailed logs for extended periods. High volumes of such requests burden courts in high technology regions such as California, which form the backbone of Internet connections.

---

[46] Security Institute, CSI/*FBI Computer Crime and Security Survey*, (2002) http://www.gocsi.com/press/20020407.html at 10 August 2002.
[47] Deposition to a Special Field Hearing Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington D.C., April 21 2000, (Special Agent Guadalupe Gonzalez) http://www.fbi.gov/congress/congress00/gonza042100.htm.
[48] 18 USC § 3121 (c)
[49] Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.
[50] Jay Lyman, *"Feds Demand New Tech Powers To Fight Terrorism"*, NewFactor Network (http://www.newsfactor.com/pearl/story/13572.html) 18 September 2001

A further jurisdictional issue occurs if the communication leaves the United States and the assistance of foreign investigators and the cooperation of foreign governments is required. The problem with this is that often some countries do not have the training, resources, or in some cases, the intention to render assistance. Some countries may not even have laws against the relevant computer intrusion.

Difficulties in Interpretation

Many of laws outlined earlier in this report that relate to computer breaches specify the need for criminal intent, *mens rea*. This creates difficulty in proving the true objective of a hacker. The ambiguity is in determining if the intention was to delete or alter files, or was this just accidental result while viewing them.[51] Another area of difficulty is in determining whether or not more than $5,000 damage was caused. It is often difficult to ascertain exactly what damage was caused and indeed quantifying this loss. This was evident in Moulton v. VC3 where Scott Moulton was acquitted of violations of 18 USC § 1030 (a)(5)(B) because of the inability to prove damages of financial loss of $5000.[52]

Inadequate Deterrence

Advocates including Congressman Herger of California, and Mark Colombell,[53] believe that the existing legislation is not strict enough to effectively deter individuals from committing computer crimes. Others including Senator Charles E. Schumer suggest that to kerb the growing rate of juvenile offences, the statute be altered to "give federal law enforcement authorities the power to investigate and prosecute juvenile offenders of computer crimes in appropriate cases".[54]

Barriers to Assistance

This point relates to the observation earlier that some network administrators do not posses a high degree of knowledge in relation to network security, a view supported by security experts.[55] 18 U.S.C. §2511 creates ambiguity at to whether or not a computer owner can seek assistance from the government to conduct monitoring for violations. Often computer owners lack the specific knowledge, skills, equipment and resources to protect themselves from attack and request assistance in monitoring their systems.[56] Because of the ambiguity caused by § 2511 law enforcement are reluctant to render assistance. This produces an anomaly whereby a "computer hacker's

[51] Dr David Cater, *Computer Crime Categories: How Techno-criminals Operate*, Michigan State University, http://nsi.org/Library/Compsec/crimecon.html .
[52] William Reilly, "Port Scanning: Is it Illegal?", The Reilly Column Online Security, http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=23 , at 11 August 2002
[53] Mark R. Colombell, "*The Legislative Response to the Evolution of Computer Viruses*", 8 RICH. J.L. & TECH. 18 (Spring 2002) at http://www.law.richmond.edu/jolt/v8i3/article18.html.
[54] Charles E. Schumer, Letter to Congress Colleagues 16 February, Centre for Democracy & Technology, http://www.cdt.ord/security/doc/000216schumer.shtml at 12 August 2002
[55] Eric Cole, SANS Security Cyber Defence Initiative, http://www.sans.org/CDI.htm at 5 August 2002.
[56] Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.

undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims."[57]

[57] Orin S. Kerr, Are We Overprotecting Code? Thoughts on First-Generation Internet Law, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Goals of a Desirable System

The presentation of the alleged defects in the previous section of this report would suggest that certain underlying goals underpin a desirable system. The ultimate goal of such a system would be to eradicate all instances of unauthorised computer intrusions, and the eradication of computer crime. Given the current situation previously outlined, this is a utopian goal, however, the road to achieving this ideal does present some more immediately achievable objectives. It would be possible to move a step closer to achieving the ultimate goal of no unauthorised computer intrusions or crime by breaking this down more into more manageable and measurable goals.

More Secure Electronic Environment

Currently the underlying technology driving Internet communication is based on IP (Internet Protocol), a connectionless protocol used to connect two or more devices over a network. The rapid proliferation of the Internet has meant that the requirements placed upon this protocol have exceeded its initial design specifications. This is evidenced by the alarming shortage of IP address in the current model of IP version 4.[58] The connectionless nature of the protocol also makes the issue of security more difficult, and indeed more fallible. The ultimate goal in this regard is to develop a universally accepted protocol that accommodates modern requirements and makes provision for anticipated and even unanticipated developments.

Increased Investigation and Prosecution of Alleged Computer Intrusions

The inference in this goal is that an increased number of investigations will yield a higher volume of prosecutions. It is hoped that increased prosecutions will act as a deterrent to potential offenders, preventing them from committing offences in the first place. Greater deterrents are a favourable goal as they provide more long-term benefits. If they are successful, deterrents will reduce the amount of cyber intrusion, achieving the primary goal, and in the longer term, reduce the burden on resources including the costs of ongoing imprisonment and rehabilitation.

[58] Rupert Goodwins, *Do we really need an IP upgrade?*, ZDNet News, http://zdnet.com.com/2100-1105-855326.html at 12 June 2002

More Effective and Powerful Legislation in the Area of Computer Intrusion

The goal of more powerful legislation is a product of the quest for increased investigation and prosecution and subsequently greater deterrents. The goal here would be to create legislation that gives more power to the investigators of alleged breaches of computer intrusions, ultimately setting forth legislation that is universal to the concepts of law and equity. Legislation should not be bound by technologically specific language and should allow for changing interpretation with advance in technology. Finally effective legislation should not infringe on the rights and privileges afforded to its citizens in the Constitution and Bill of Rights.

Options for Change

Developing options for change for the reduction of computer intrusions is problematic. Because the Internet, and associated technologies, are such a new and rapidly developing area, the scope of choices is limited. Options for change in relation to the Internet framework are currently under debate globally. Such debates are subject to the challenges created by the borderless nature of the Internet. One option for change would be to develop a controlling body that would create new standards for implementation of Internet based technology. This body would then be empowered to adopt, and enforce, single standards that make the underlying infrastructure of the Internet more applicable to the current requirements of its uses.

Options for change in relation to legislation surrounding the issue of computer intrusion, and the broader field of cyber crime, are likewise difficult to establish. Again due to the relative infancy of the Internet, there are few bases for comparison. Some countries do not even posses specific legislation in relation to cyber crime. It can be argued that the United States currently has one of the most developed and comprehensive arrays of laws and regulations relating to the Internet. It is difficult then to compare the situation of the United States with examples of other legislation around the world. The United States is somewhat of a pioneer in the area of cyber law. Changes to existing laws and the development of new laws have no benchmark against which to assess the extent which the new cyber laws meet the goals of the system. Developing new and altering existing laws in relation to computer intrusion is another option for achieving the goals in reducing, and hopefully eradicating computer intrusion.

A further option to address the issue of computer intrusion is to increase the deterrence of this crime, making it less appealing to current and potential offenders. One method of achieving this is to develop tougher penalties for offenders, as well as increase the ability to investigate and prosecute offenders. Changing existing legislation relating to computer breaches, as discussed previously, and increasing the effectiveness of investigators might facilitate this objective. More resources should be allocated to the investigation of alleged offences. Resources include time, skilled investigators, high end sophisticated computer hardware and associated software and the ability to access information required to process and investigate, coupled with increasing levels of education. Education of the broader community may be of assistance in the fight to increase deterrence and hopefully reduce the prevalence of cyber intrusion. Education of system administrators may also serve to achieve reduced computer intrusion. If systems were more secure and consequently it were more difficult to gain access in the first place, this could also act as a deterrent, even an obstacle to some offenders.

Necessary Actions for Change

The option of updating the current underlying framework of the Internet requires the development of a clear and unchallenged Internet governing body. Currently a great deal of disagreement exists over the accreditation of administering bodies that would be qualified to regulate and govern the Internet. One controlling body could allow changes to occur to protocols such as IP as well as a host of other protocols vastly used on the Internet. A single body would be required to adopt and make adjustments to this standard. Currently Internet Standards are only guidelines, and adoption is not mandatory. A single officiating body could change this. Such a body would have to be empowered to establish an appropriate and effective framework, but would also have to ensure that it was adopted universally. It is reasonable to assume that such a body would be required to assist in the transition by way of education, and support, both financially and physically. The infrastructure of the Internet would need to change to adopt the new framework, as would the individual machines that form the Internet. All devices, new and old, would have to be compliant with the new infrastructure. For a new framework to be implemented it would require the support of the whole Internet community.

In regards to the second option for change, alteration of the governing laws and statutes, the necessary actions required are more easily identified. The due process of adding or changing the law revolves around the support of the elected members of the government. These members are the elected representatives of the people of the United States. Proposed statute must receive due process through the US House of Representatives, the Senate and finally the President of the United States. Intense lobbying by interest groups usually accompanies any legislative proposals. The action required to increase the investigation and subsequent prosecution of computer intrusion would require the allocation of more financial resources. This is also the case for increased education. Increased financial resources almost always require the due process of the government. Significant political or social pressure can serve as a catalyst in this process. In regards to the passing of the USA Patriot Act into law, significant pressure and support resulted from the September 11 attacks on the United States. The emotion and motivation of the people allowed for the very prompt passing of the Act.

Analysis of Alleged Advantages and Disadvantages

Restructure Internet Framework

This option requires the reengineering of the fundamental building blocks of the Internet standard for communication. It would involve the appointment of an officiating body to control and oversee the transition, and to administer proposed changes to the adopted standard. There would be many benefits to partaking in such an activity. Firstly the appointment of a single controlling entity would provide some clarity and consistency in the continued development of the Internet. A universal standard would also allow for the widespread adoption of a standard such as IPv6 which would also solve the additional conundrum of the rapidly depleting pool of available Internet addresses[59]. This in its self would have many benefits with the greater increase of wireless devices and projected growth of computers expected to continue to escalate rapidly.[60] A new standard could include a provision for security built into the underlying protocol instead of building security around the protocol. This basically means that network communication would be more secure than current configurations allowing verification to be built in, which would make it increasingly difficult to intercept communications in transit. Security provisions could also be used to identify and verify users.

While there are some positive advantages in restructuring the Internet configuration, there some very real disadvantages as well. Firstly there is the difficulty in deciding the composition of the necessary officiating body. The borderless nature of the Internet has made it difficult to determine exactly who should be on such an organisation, more importantly who should lead it. Difficulty has already arisen in a similar matter dealing with the provision of domain name allocations, and appointing registrars.[61] Already there exists a host of Internet organisations including: ICANN, ISOC, ITEF, IAB and W3C. Each of these already has its fair share of difficulty deciding upon its own leadership. Since the terms of reference of the body would need to be universally accepted, the Internet community would have to acknowledge this governing body. The next disadvantage is the total cost of this exercise. To make every device on the network compatible, each would have to be upgraded. While this may just be a matter of updating the software components, there would still be some degree of downtime. The cumulative cost of this downtime, even if it were only for an hour or two would be astronomic to attempt to predict.

Updating the framework that underpins modern communication would provide many improvements in security. Inbuilt security may hinder the ability of some hackers, including a growing number of script kiddies, but it doubtful that this option would stop the proliferation of computer penetration.

---

[59] *"Introduction to IV Version 6"*, Microsoft Publications, (http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/introipv6.asp) 14 February 2002.

[60] "IPv6: an Internet Protocol for the Future", The Butlet Group, (http://www.serverworldmagazine.com/opinionw/2002/04/25_ipv6_shtml) 25 April 2002.

[61] Bret Fausett, Governing a Global Resource from Los Angeles County, WebTechniques, http://www.newarchitectmag.com/archives/2002/01/legal/ , at 3 August 2002.

USA Patriot Act of 2001

The USA Patriot Act of 2001 was enacted a blistering five weeks after the first version was introduced to the House for discussion. The bill is some 342 pages long and amends over 15 different statutes.[62] The third and final version of the bill was passed 357-66 in the House[63], and 98-1 in the Senate[64] before being signed off on by President George W. Bush 26 October 2001. The act covers a wide range of topics including: providing for the victims of terrorism and public safety officers, enhanced domestic security and surveillance, money laundering and anti-terrorist financing, boarder protection, removal of obstacles to investigating terrorism, increased information sharing for critical infrastructure, improved intelligence, strengthening the criminal laws against terrorism and some other miscellaneous inclusions.[65] While this is a comprehensive list, for the purpose of this report the section relating specifically to computer intrusions will be evaluated. The act as a whole will not be assessed on alleged benefits and disadvantages but rather the relevant sections will be addressed.

Changes to 18 U.S.C §1030 Computer Fraud and Abuse Act

The majority of the changes that occur to this act as a result of the USA Patriot Act are noted under § 814 relating to Deterrence and prevention of cyberterrorism. It should be noted at this juncture that violators of 18 USC §1030(a)(1), illegally accessing computer identified as requiring protection, or 18 USC §1030 (a)(5)(A)(1), (which will be discussed shortly) as offences that may constitute a federal terrorism.[66] As per 18 USC 2332b (g)(5)(B) classification of a federal terrorism offence entitles the use of more stringent penalties, pre conviction seizure of assets and penalties of those deemed to be harbouring or aiding, among others.[67] Potential classification of these acts as terrorist offences also means that more aggressive methods of surveillance may be used; this is examined in more detail in the next section.

As stated in the current events section of this report to violate 18 USC (a)(5)(A) a violation had to "intentionally cause damage" which was defined as an impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating at least $5,000 in value, interferes with medical treatment diagnosis or care, or causes physical injury to any one person or threatens public safety.[68] USA Patriot act § 814 moves everything after "…a system, or information" into the offence and adds to them "damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defence, or national

---

[62] *EFF Analysis Of The Provisions Of The USA PATRIOT Act*, (http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html) , 31 October 2001.
[63] Declan Mc Cullagh, *USA Act Stampedes Through*, Wired News, (25 October 2001) http://www.wired.com/news/conflict/0,2100,47858,00.html, at 8 November 2001.
[64] Declan Mc Cullagh, *Spying: The American Way of Life*, (11 March 2002) Wired News, http://www.wired.com/news/conflict/0,2100,47858,00.html, at 3 April 2002.
[65] *USA Patriot Act,* Pub L No 107-56, §§ 1-1016, 115 Stat. 272 (2001).
[66] *USA Patriot Act,* Pub L No 107-56, §808, 115 Stat. 272 (2001).
[67] *EFF Analysis Of The Provisions Of The USA PATRIOT Act*, (http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html) , 31 October 2001.
[68] 18 USC § 1030 (e)(8)

security"[69]. This means that if a violation occurs and the government can not prove $5,000, this is still a federal offence.

As a result of moving the definition into the offence, damage is amended and defined as, "any impairment to the integrity or availability of data, a program, a system, or information".[70] This removes some of the ambiguity referred to in difficulties of interpretation section of this report. Special Agent Gonzales of the FBI also raised such difficulties.[71] In the amended configuration there is still a requirement to prove *mens rea*. It is hoped that this will remove the confusion as to whether the intention was to cause $5,000 worth of damage, but rather the intention of damage, as defined above.[72] These changes are advantageous in achieving the goal of more clear and powerful legislation, removing ambiguity. A further advantage is the broadening of the act to extent possible violations, extending the reach of this statute. From a negative perspective, it could be perceived by civil libertarians that the broadening of 'damage' definition allows wider classification of (a)(5)(A)(1), where an offence may be classified as a terrorist act. As mentioned previously in this section, terrorist offences entitles the government to more invasive measures of surveillance, which some civil libertarian groups find contentious.[73]

18 USC § 1030 was further altered in subsection (c) relating to penalties. Penalties have doubled for offenders to §1030(a)(5), which, according to the text above, were redefined to damaging a protected computer. First time offenders or (a)(5)(A)(i) now receive 10 years maximum prison, (a)(5)(A)(ii) remains at 5 years, while repeat offenders to either of these receive 20 years maximum. These extended sentences have the alleged benefit of serving as additional deterrent. One negative impact of the increasing sentence is that those convicted will place a larger burden on the penal system, with the Department of Corrections requiring more resources to uphold the sentence. In this instance it is felt that the positive impacts far outweigh the negatives. It may be argued that such an increase would only be short term as the longer term effects of reduced offences are hopefully reduced over time due to deterrence.

The USA Patriot Act also makes a change to the definition of protected to include "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[74] This definition greatly alters the jurisdiction of the United States. Under this new definition any person who penetrates a computer that is used by United States trade or commerce has committed an offence under United States federal law. This can apply to individuals not even in the United States. A link can be drawn to suggest that use of the Internet constitutes interstate or foreign commerce simply because it utilises phone

---

[69] *USA Patriot Act,* Pub L No 107-56, §814(a)(4)(B)(v), 115 Stat. 272 (2001).
[70] 18 USC 1030 § 1030 (e)(8)
[71] Deposition to a Special Field Hearing Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington D.C., April 21 2000, (Special Agent Guadalupe Gonzalez) http://www.fbi.gov/congress/congress00/gonza042100.htm.
[72] Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.
[73] *USA Patriot Act Boots Government Powers While Cutting Back on Traditional Checks and Balances*, (http://www.aclu.org/congress/l110101a.html), 4 November 2001.
[74] *USA Patriot Act,* Pub L No 107-56, §814 (d)(1), 115 Stat. 272 (2001).

lines[75]. Thanks to this definition the United States could, by all rights, prosecute a hacker that routed communications through a US switch or router even if he/she or the target are not even located within the United States. The Department of Justice claims it has the power to prosecute such a case but lacks the intention.[76] This has a positive outcome in the area of deterrence, not only hopefully reducing internet intrusions in the United States but globally. This also moves towards the goal of education. United States investigators may now be forced to cooperate with foreign investigators to allow education about the methods and issues related to computer intrusions. The United States will also be able to step in and assist with international cases. There are some disadvantages in this change. Some nations may resent this move as an erosion of territorial sovereignty. In may be seen a move to allow the United States to make a bid for the controllership of the Internet. A further disadvantage is that should countries begin calling for the assistance of the United States that this will place a large burden on the US resources.

Under changes to the definition of conviction, the classification is amended to include conviction under state law relating to unauthorised access. If an individual has been convicted at state level, they are eligible for the larger prison term provided under 18 USC §1030 (c). Greater deterrents for repeat offenders will exist and eventually reduce the incidence of computer intrusions.

Previously under § 1030 there was no definition of loss. In United States v. Middleton[77] it was held that loss could include responding to the offence, damage assessment, disaster recovery and lost revenue because of intrusion.[78] This decision was codified under the USA Patriot Act §814 (d)(11). Civil restitution for breaches of this act will be easier to claim rendering the legislation more effective and creating a further deterrent. While this is true for criminal matters, the damage in civil proceeding is limited to economic damages. Further to this, loss does not include negligent design or manufacture. This inclusion might serve well to limit the application of this section beyond computer fraud and abuse that may burden the legal system.

Finally USA Patriot Act §814 (f) sees the abolition of mandatory minimum sentences in all instances of this section. This could be of disadvantageous in relation to the removal of some element of deterrent. It could be suggested that with all the previous positive elements relating to deterrence, this is not a large issue. This alteration does not suggest a reduction in any way, just an element that would mandate definite prison sentence in all cases of conviction.

---

[75] Developers Should Beware of the Economic Espionage Act, Poznak Law Firm LTD, http://www.poznaklaw.com/articles/econoespionage.htm at 14 August 2002.
[76] Mark Rasch, *Ashcroft's Global Internet Power- Grab,* Security Focus Online, http://online.securityfocus.com/columnists/39 at 30 June 2002.
[77] United States v. Middleton 231 F.3d 1207, 1210-11 (9th Cir. 2000)
[78] Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.

Resource Allocation Assisting Computer Intrusion

§ 101 Counterterrorism Fund

This section makes provision for the allocation of funds by the government for the purpose of counterterrorism activities. This section is related to computer intrusion as some acts of intrusion classify as terrorism offences. Specifically of interest is the availability of funds to pay rewards relating to countering, investigating or prosecuting domestic or international offence. Such a provision, if applied to computer intrusion, may act as a catalyst to investigations. Informants may be more forthcoming it they believe they may be rewarded. The disadvantage is that no mention is made about who approves and administers this fund. It appears that currently this fund could be exploited.

§ 105 Expansion of National Electronic Crime Task Force

This section directs the Secret Service, one of the investigating bodies of 18 USC §1030, to establish a national network of electronic crime task forces. This will enhance the prevention, detection and investigation of electronic crime. This provision has fantastic benefits for the investigation of cyber intrusion, as well as other cyber crime. This will allow the purchase of required equipment, provision of resources for the purpose of training and educating law enforcement officials in more efficient means of processing specialised investigations. This may also allow the agency to hire investigators at the more professional end of the market. A possible disadvantage is that the funding may not be shared with the FBI who some legislation state are responsible for investigation of certain computer intrusion related offences.[79]

Surveillance Activities Assisting in the Investigation of Computer Intrusion

§ 217 Interception of Computer trespasser communication

This act authorises a computer owner to request assistance for monitoring their systems. This is subject to the owner of the 'protected computer' must authorise the interception of information.[80] The person intercepting the communication must be lawfully engaged in an ongoing investigation.[81] 'Reasonable grounds' to believe that the contained information relevant to the ongoing investigation must exist.[82] Finally interception must only contain communications to and from the computer trespasser.[83] Computer trespasser is defined to deliberately exclude individuals known by the owner to have access to all or part of the computer.[84] This would exclude instances like university campuses where students have some form of access by way of an account. This provision expires 31 December 2005. This provides an advantage as it allows some network administrators the opportunity to develop more of an education

[79] 18 USC § 1030 (c)(4)(D)(2).
[80] 18 USC § 2511 (2)(i)(I)
[81] 18 USC § 2511 (2)(i)(II)
[82] 18 USC § 2511 (2)(i)(III)
[83] 18 USC § 2511 (2)(i)(IV)
[84] Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.

in relation to security issues. It also allows greater enforcement and application of the statue while at the same time creating deterrence. However, this provision allows for exploitation by the government with such lenient terms as 'reasonable ground to believe'. Additionally this element is not supervised by any court or additional body.

§ 219 Single-Jurisdiction Search Warrants for Terrorism

As discussed earlier, some computer intrusion offences can be classified as terrorism offences. As such these offences would fall under §219 that allows a judge in any district to issue a search warrant that can be exercised anywhere under United States jurisdiction. This search allows for the search of property and persons. This provision does not expire in 2005. If used in conjunction with § 213 notification of the exercise of the warrant may be delayed if the court finds that immediate disclosure may have an adverse affect. This is also called a sneak and peek order. Such an order is less pertinent to computer intrusion as this section prohibits the seizure of any wire or communication equipment. It does not. This may have the alleged benefit of enhancing the power of investigators and hopefully by iteration, increase prosecutions and hence reduce incidence of computer intrusion by iteration.

§ 216 Pen Register and Trap and Trace Statute

The main alteration of this statute renders it more relevant to modern communication. Much of the telephone specific information has been altered to include terms relevant to computer communication and cellular communication. The changes also make reference to the evolving method of performing surveillance with software not necessarily hardware that would need to be attached.[85] This is advantageous, making the law more relevant and applicable to modern events and methods. § 216 also allows for the provision of nationwide effect of pen trap orders. This eases the burden on districts with high proportions of technology infrastructure. It also allows for faster and hence more efficient access to the required information. There is less chance that the information will be discarded as a result in delays obtaining orders. Conversely this removes many of the checks and balances in the obtaining the order in the first place, rendering it more vulnerable to abuse and difficult to detect.

§ 220 Nationwide Search Warrants for Email

This provision allows for the single jurisdiction of search warrants in relation to email. Providers beyond the jurisdiction of the issuing district can be served with these orders. This rule only applies to email less than six months old. This section provides similar benefits and disadvantages as the previous section relating to Pen Register and Trap Trace Statute.

[85] Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.

Evaluation of Adopted Option for Reducing Computer Intrusion

The passing of the USA Patriot act identifies the choice of the United States government in dealing with the problems associated with computer intrusion. I would concur with the evaluation of the United States legislators in choosing this option over the alternative suggested in this report. It is agreed that the adoption of a single governing body to regulate and redesign the specification of Internet computer infrastructure would have its share of benefits. It is doubtful that this option would greatly assist in the move towards achieving the ultimate goal of little to no incidence of computer intrusion. Given this presumption it is unclear that the benefits far outweigh the costs of implementing this option.

The option of altering the legislation provides for a more measurable, and effective method of fighting computer intrusion and the broader issue of cyber crime. The changes brought about in the adoption of the USA Patriot act address many of the pre-Patriot legislative issues identified earlier in this report. The act deals with jurisdictional issues, addressing language to make the law more up to date with technological advancement removing some of the difficulties in interpretation. The legislative changes also reduce the barriers of government assistance. The changes combined with greater resources granted in the USA Patriot Act form a greater deterrence to current and potential computer intruders. This deterrence is augmented by the additional powers of investigators afforded by the Patriot Act. These additional powers also have some disadvantages also.

Civil libertarians claim that some portions of the Patriot act are "draconian"[86] The negative sentiment of the broad sweeping powers of investigators and intelligence gathers were reflected in a statement made by Laura Murphy, Director of the national office of the American Civil Liberties Union. "This law is based on the faulty assumption that safety must come at the expense of civil liberties."[87] While these new provisions for surveillance are somewhat less restrictive than pre-Patriot laws they do greatly alter the ability to investigate and hopefully prosecute offenders of computer intrusion. While this may come at the perceived expense of some constitutional rights, the majority of the more controversial provisions do 'sunset' or expire on 31 December 2005. This will allow the law maker to review and re-evaluate the cost benefit of these laws. From the perspective of investigating and prosecuting computer intrusion, the legislative changes provided in the USA Patriot Act represent an effective and beneficial option for the reduction and eradication of computer intrusion and cyber crime.

---

[86] *USA Patriot Act Boots Government Powers While Cutting Back on Traditional Checks and Balances*, (http://www.aclu.org/congress/l110101a.html), 4 November 2001.
[87] Laura Murphy, *USA Patriot Act Boots Government Powers While Cutting Back on Traditional Checks and Balances*, (http://www.aclu.org/congress/l110101a.html), 4 November 2001.

Measuring the Outcome

Given the relative infancy of the USA Patriot Act, it is moderately difficult to measure the effectiveness of the measures aimed at the reduction of computer intrusion. There also exists another element of difficulty in the measurement. Much of the activity related to the Patriot Act is closely correlated with terrorism and terrorist offences. As such, some of these issues are classified materials as they relate to national security. This means that much of the information may not be available for public scrutiny or evaluation. There are limited checks and balances on the individuals that are able to use this act to investigate and prosecute the relevant crimes. The only public measure of the effectiveness is the number of prosecutions relating to computer intrusion, and the figures of actual incidence of computer intrusion similar to those released in the FBI/ CSI Computer Crime and Security Survey.

Preliminary reports indicate that these new measures are in fact reducing the incidence of computer crime. One analyst cites the increased prison sentences afforded in the Patriot Act for the recent decline in the proliferation of computer viruses.[88] Speaking at DefCon an annual hacker conventions, security specialist 'Simple Nomad' commented "What was once a misdemeanour pre-Patriot Act could be a felony now with a five – to 1o year sentence…That scares a lot of people."[89] Although these are not conclusive results, they do give the impression that perhaps the Patriot Act has been successful in increasing deterrents to computer offences. This was one of the goals outlined in the report to overcome some of the alleged deficiencies of the pre-Patriot legislation.

Groups including the Electronic Frontier Foundation are calling for the courts to appropriately punish those that misuse the powers of surveillance afforded by the Patriot Act[90] The problem is that often the courts are unaware of the full extent of what is happening due to the abolishment of the pre-existing checks and balances. Additionally the EFF and other groups are urging congress to demand reports on the use of the clauses that are set to 'sunset' on 31 December 2005 so that an informed decision can be made on the ongoing viability of these laws.

---

[88] Reuters, *New computer security dilemma: a lack of viruses*, SiliconVally.com, (http://www.siliconvaley.com/mld/business/special_packages/security/3848828.htm) at 14 August 2002.

[89] Elinor Abreu, Stakes Higher for Hackers After Sept. 11, Reuters, (http://story.news.yahoo.com/news?tmpl=story&u=?nm/20020811/tc_nm/hackers_dc_2) at 15 August 2002.

[90] *EFF Analysis Of The Provisions Of The USA PATRIOT Act*, (http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html), 31 October 2001.

Conclusion

While there is only preliminary supporting evidence, it would be fair to assume that the introduction and implementation of the USA Patriot Act will achieve a reduction in the overall incidence of cyber crime, but more specifically computer intrusion. The act makes provisions for increased access to resources to assist in the prevention of cyber crime.[91] This coupled with increasing powers of surveillance and investigation provides more force and effectiveness in the processing of alleged breaches of cyber crime. Larger scope in the classification of breaches of the law, as well as more severe penalties for infringements make offences much more serious under this new legislation. The act also alters some of the language used in the existing statutes making the law more up to date and hence more useful in the prosecution of computer breaches. The classification of certain computer intrusion offences as act of terrorism adds further deterrence. Acts of terror enlarges the penalises applied to offenders, and indeed those who aid such people. The combination of all these elements equate to a clear signal that the Government of the United States considers computer intrusion to be a most serious offence. The changes are a clear signal that offenders are susceptible to severe and real punishment for their actions. It is hoped that the changes provided in the USA Patriot Act of 2001 will act as a significant deterrent, and greatly reduce the incidence of computer intrusion allowing users of the Internet renewed confidence in the integrity of their information and the continued growth of Internet technologies.

[91] *USA Patriot Act,* Pub L No 107-56, §105, 115 Stat. 272 (2001).

Bibliography

Legislation

18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices

18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers

18 U.S.C. § 1362. Communication Lines, Stations, or Systems

18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited

18 U.S.C. § 2701. Unlawful Access to Stored Communications

18 U.S.C. § 2702. Disclosure of Contents

18 U.S.C. § 2703. Requirements for Governmental Access

18 USC § 1362 Communication Lines Stations, or Systems

18 USC § 3121 Definitions

Crime control Act of 1990, 42 U.S.C.A. §13032

USA Patriot Act, Pub L No 107-56, 115 Stat. 272 (2001)

Case Law

United States v. Middleton 231 F.3d 1207, 1210-11 (9th Cir. 2000)

Articles/ Books / Reports

Bret Fausett, Governing a Global Resource from Los Angeles County, WebTechniques, http://www.newarchitectmag.com/archives/2002/01/legal/ , at 3 August 2002.

Dan Verton, *The Hacker Diaries Confessions of Teenage Hackers*, McGraw-Hill (2002) 195.

David Johnson and David Post, 'Law And Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367, IB http://www.cli.org/X0025_LBFIN.html

Declan Mc Cullagh, *USA Act Stampedes Through*, Wired News, (25 October 2001) http://www.wired.com/news/conflict/0,2100,47858,00.html, at 8 November 2001.

Dr David Cater, *Computer Crime Categories: How Techno-criminals Operate*, Michigan State University, http://nsi.org/Library/Compsec/crimecon.html

Elinor Abreu, Stakes Higher for Hackers After Sept. 11, Reuters, (http://story.news.yahoo.com/news?tmpl=story&u=?nm/20020811/tc_nm/hackers_dc_2) at 15 August 2002.

Henry Lee, *Hacker Stole Thousands Of Passwords UC Berkeley case shows access flaws,* San Francisco Chronicle, http://www.sfgate.com/cgibin/article.cgi?file=/chronicle/archive/1998/08/13/MN26139.DTL 13 August 1998

Jay Lyman, *"Feds Demand New Tech Powers To Fight Terrorism"*, NewFactor Network (http://www.newsfactor.com/pearl/story/13572.html) 18 September 2001

Lasse Huovinen, Jani Hursti, *Denial of Service Attacks: Teardrop and Land*, Department of Computer Science Helsinki University of Technology http://www.hut.fi/~lhuovine/hacker/dos.htmhttp://www.hut.fi/~lhuovine/hacker/dos.htm , at 3 August 2002.

Mark R. Colombell, "*The Legislative Response to the Evolution of Computer Viruses*", 8 RICH. J.L. & TECH. 18 (Spring 2002) at http://www.law.richmond.edu/jolt/v8i3/article18.html.

Mark Rasch, *Ashcroft's Global Internet Power- Grab,* Security Focus Online, http://online.securityfocus.com/columnists/39 at 30 June 2002.

Maury Shenk, "Should a Corporation Report a Breach to Law Enforcement?", [volume 1], Secure Business Quarterly, http://www.sbq.com/sbq/digital_forensics/sbq_forensics_reporting_breachs.pdf [pps 4-6]

Orin S. Kerr, Are We Overprotecting Code? Thoughts on First-Generation Internet Law, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Rebecca Sausner, *"U.S., Chinese Hackers Wage Quiet War"*, Newsfactor Network, (http://www.newsfactor.com/perl/story/9203.html) 24 April 2001.

Reuters, *New computer security dilemma: a lack of viruses*, SiliconVally.com, (http://www.siliconvaley.com/mld/business/special_packages/security/3848828.htm) at 14 August 2002.

Rupert Goodwins, *Do we really need an IP upgrade?*, ZDNet News, http://zdnet.com.com/2100-1105-855326.html at 12 June 2002

USA Patriot Act Boots Government Powers While Cutting Back on Traditional Checks and Balances, (http://www.aclu.org/congress/l110101a.html), 4 November 2001.

William Reilly, "Port Scanning: Is it Illegal?", The Reilly Column Online Security, http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=23 , at 11 August 2002

Other Sources

"Introduction to IV Version 6", Microsoft Publications, (http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/introipv6.asp) 14 February 2002.

Charles E. Schumer, Letter to Congress Colleagues 16 February, Centre for Democracy & Technology, http://www.cdt.ord/security/doc/000216schumer.shtml at 12 August 2002

Clinton William, "Executive Order 13133" (The White House Washington D.C. , August 5 1999) http://resource.lawlinks.com/Content/Legal_Research/Executive_Orders/1999/Technology/executive_order_13133.htm

Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.

Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, (2002), Department of Justice, http://www.cybercrime.gov/PatriotAct.htm at 10 June 2002.

Computer Security Institute, CSI/*FBI Computer Crime and Security Survey*, (2002) http://www.gocsi.com/press/20020407.html at 10 August 2002

Deposition to a Special Field Hearing Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington D.C., April 21 2000, (Special Agent Guadalupe Gonzalez) http://www.fbi.gov/congress/congress00/gonza042100.htm

Deposition to Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary and Related Agencies, Washington D.C., 16 February 2000, (Louis Freeh) http://www.fbi.gov/congress/congress00/cyber021600.htm .
Deposition to Senate Judiciary Committee Criminal Justice Oversight Subcommittee and House Judiciary Committee Crime Subcommittee, Washington D.C., February 29 2000, (Michael A. Vatis) http://www.fbi.gov/congress/congress00/vatis022900.htm

Developers Should Beware of the Economic Espionage Act, Poznak Law Firm LTD, http://www.poznaklaw.com/articles/econoespionage.htm at 14 August 2002.

EFF Analysis Of The Provisions Of The USA PATRIOT Act, (http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html) , 31 October 2001.

Eric Cole, SANS Security Cyber Defence Initiative, http://www.sans.org/CDI.htm at 5 August 2002.

Laura Murphy, *USA Patriot Act Boots Government Powers While Cutting Back on Traditional Checks and Balances*, (http://www.aclu.org/congress/l110101a.html), 4 November 2001.

President's Working Group on Unlawful Conduct on the Internet, United States Presidential Authority, *The Electronic Frontier: The Challenge Of Unlawful Conduct Involving the Use of the Internet*, (March 2000), Section I

Reno Janet, "Keynote Address" (National Association of Attorneys General, Stanford Law School California, 10 January 2000)
http://www.usdoj.gov/opa/pr/2000/January/007ag.htm

Security Institute, CSI/*FBI Computer Crime and Security Survey*, (2002)
http://www.gocsi.com/press/20020407.html at 10 August 2002.

Spectrum Systems, The Why's, What's, Who's and How's of Network Security, (2002), http://www.spectrium-systems.com/wp_security_basics.htm at 11 August 2002