TOWARD A MORE EQUITABLE PROSECUTION OF CYBERCRIME: CONCERNING HACKERS, CRIMINALS, AND THE NATIONAL SECURITY

INTRODUCTION

When I was fifteen and in tenth grade, on the first Friday of every month, I used to tell my mother I was engaged in some sort of after-school activity and would not be home until late that evening. Instead of engaging in that activity, I took the school bus as close as possible to the train station. I would then take the 3:06 p.m. train from Ronkonkoma, New York—the last stop on Long Island—to Pennsylvania Station, New York City. From Penn Station, I took the "F" Train uptown to 53rd and Lexington. From Lexington, I walked over to 3rd Avenue to what was then called the Citicorp building.[1] I would glide down the escalators of the Citicorp building to where fast-food chains surrounded the lobby and a large bank of payphones stood. In the lobby of the Citicorp building, on 53rd and 3rd, next to the payphones, the first Friday of every month, at five o'clock, was where the New York 2600 Meetings took place. This is where the hackers met.

It was always a motley group. There were many teens wearing baggy black clothes, toting bags with arcane electronic equipment, radio frequency scanners, magnetic strip readers and writers, laptops, and mysteriously misappropriated telephone-company equipment. There was an older contingency who spoke of the days of yore when the telephone system operated on analog switches and blueboxing was commonplace.[2] There were gentlemen in suits selling digital crystals, at an inflated price, that would allow one to construct a redbox.[3] Like clockwork, a phone phreak[4] from Australia, who used the alias "Phoney," would call the Citicorp lobby's payphones just to chat with the New York hackers, and would

---

1. In 1998, Citicorp and Travelers Group merged, forming Citigroup. Citigroup, *Citigroup and Travelers Group to Merge, Creating Citigroup: The Global Leader in Financial Services*, *available at* http://www.citigroup.com/citigroup/press/1998/980406a.htm (Apr. 6, 1998).

2. Blueboxing refers to the practice of sending a 2600 cycle tone into the mouthpiece of a telephone thereby allowing the user, with the addition of four touchtones, to become the equivalent of a telephone-company operator. *See* http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci212783,00.html (detailing commonly used terms of the computer underground and computer security world, and discussing blue boxes under the definition of "phreak") (last visited May 14, 2005).

3. A Redbox is the colloquial name for a device that replicates the beeping sound a payphone sends to the telephone switch computer whenever a customer places a quarter in a payphone; replicating this sound allowed one to place phone calls without pay. *See id.* (discussing red boxes under the definition of "phreak").

4. Phone phreaks are much like computer hackers, except that their main interest lies in the machinations of the telephone system. *Id.*

invariably brag of a curious device he constructed that obviated the need to pay for payphone calls by administering a high-voltage electric shock to the payphone itself.

More than anything else, the attendees exchanged knowledge. The attendees of the New York 2600 Meetings were some of the brightest and most inquisitive minds that I have ever met. Unfortunately, authorities considered much of the knowledge traded between attendees dangerous and illegal. Therefore, computer hackers and phone phreaks were not the only attendees of the meetings: law enforcement conspicuously tried to inconspicuously monitor many meetings.

The Computer Fraud and Abuse Act of 1984 charged the Secret Service with the responsibility and authority of investigating computer crime.[5] Not surprisingly, undercover Secret Service agents became frequent attendees and tacit, unwilling participants to computer hacker humor. A favorite pastime at 2600 Meetings was playing "Spot the Fed," a game which does not require further explanation. In one notable and much publicized incident, photographs of a Secret Service Agent picking his nose surfaced at a 2600 Meeting and later found their way onto Fox News.[6] Shortly thereafter, in 1992, the Secret Service raided the 2600 Meeting in Virginia, at the Pentagon City Mall, and seized, detained, and in some instances, confiscated the possessions of approximately thirty attendees.[7] Such occurrences became par for the course. I made some very close friends at the 2600 Meetings, and, in the years to come, I would see a number of them sent to prison. Ten years have passed since I religiously attended 2600 Meetings, and much has changed. In our time when national security and terrorism are very real and pressing concerns, so too is the threat of a potentially devastating cyberattack on the nation's information infrastructure. Accordingly, our criminal laws and their underlying policies should justly reflect such pressing concerns.

Part I of this Note examines the first major crackdown on computer-related criminal activity, looking towards the interests protected and the chosen means of enforcement. Part II examines how various states approach the issue of computer crimes by weighing and assessing their relative successes. Part III addresses why and recommends when law enforcement ought to prosecute computer crimes, taking into account various interests and policy considerations as well as recent statutory

---

5. Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030(d) (2000).

6. 2600 Magazine, *Secret Service Photo Album*, *at* http://www.2600.com/secret/more/photo.html (last visited May 14, 2005).

7. Robert O'Harrow, Jr., *Hackers Allege Harassment at Mall*, WASH. POST, Nov. 12, 1992, at A1.

constructions. In conclusion, this Note recounts methods for the more sensible prosecution of computer crimes in the United States.

I. THE FIRST CRACKDOWN—OPERATION SUNDEVIL

On May 8, 1990, the most sweeping computer-crime crackdown to date occurred, unprecedented in scope and publicity.[8] It was known as Operation Sundevil.[9] The investigation was not directed towards intrusions of federal-interest computers, national security, or other such lofty state interests.[10] Rather, Operation Sundevil sought to combat the "traditional scourges of the [then] digital underground: credit card theft and telephone code abuse."[11] What is more, Operation Sundevil did not explicitly pursue particular egregious offenders[12]—it targeted Bulletin Board Systems ("BBSs").[13]

Before full access to the Internet was commonplace, a principal means of communication and information exchange between computer enthusiasts was through BBSs.[14] As the name implies, BBSs functioned much like an actual bulletin board, but with the addition of interactive elements.[15] A systems operator or "sysop" operated a BBS and stored the BBS entirely on a hard drive.[16] Users of the BBS would dial into the sysop's computer by modem and log into the BBS, usually under a pseudonym or handle.[17] Once logged on, a user could discuss any topic and communicate by way of

---

8. BRUCE STERLING, THE HACKER CRACKDOWN 153 (1992).

9. *Id.*

10. *See id.* (stating that Operation Sundevil did not intend to combat hacking of telephone company switching systems, software, or proprietary documents).

11. *Id.* at 154.

12. *See id.* (describing Operation Sundevil as "lack[ing] the frantic pace of the war on the Legion of Doom").

13. *Id. See generally* The BBS Corner, *An Introduction to BBS Systems*, *available at* http://www.dmine.com/bbscorner/bbsintro.htm (last modified Jan. 1, 2005) (providing a general overview of BBS systems).

14. *See* Jonathan Gilbert, Note, *Computer Bulletin Board Operator Liability for User Misuse*, 54 FORDHAM L. REV. 439, 442–45 (1985) (discussing how BBSs operate and their methods of communication).

15. United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990).

> A [BBS] is a computer program that simulates an actual bulletin board by allowing computer users who access a particular computer to post messages, read existing messages, and delete messages. The messages exchanged may contain a wide variety of information, including stolen credit card numbers, confidential business information, and information about local community events.

Id.

16. *See* Eric C. Jensen, Comment, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COMM. L. J. 217, 217–19 (1987) (describing briefly the operations of a BBS).

17. *Id.* at 223 n.41.

electronic mail to other users of the BBS.[18] BBSs became the digital equivalent of the computer underground's town square. BBS users traded information on discussion boards, circulated private e-mails, and uploaded and downloaded various types of files with ease.

BBS users developed many bulletin boards for entirely legitimate purposes. Computer users traded shareware software on a regular basis and computer enthusiasts could chat with each other regarding esoteric technical subjects that people do not often discuss in common parlance.[19] However, sysops often started BBSs with far-less-innocuous aims.

The BBSs of the computer underground were selective places of the digital elite. Simply obtaining the telephone numbers of such BBSs was an arduous task in itself and closely guarded secrets.[20] Even if one could uncover the telephone number for an elite underground BBS, that in no way guaranteed admission.[21] Sysops and members of a BBS devised elaborate schemes and tests to keep out those who had no business with the BBS, those who could not contribute to the exchange of information on the BBS, and especially to keep out law enforcement, who would, of course, ruin the fun for everyone.

Often a new user logging onto an elite underground BBS would have to know the New User Password (NUP).[22] After entering the NUP, the new user would then have to answer a series of questions.[23] Such questions often required the applicant to explain esoteric acronyms of the computer underground, frequently of a technical nature. These questions were highly specialized such that an ordinary computer user would never know the answers.[24] Even if a new user passed this rigorous test with flying colors,

---

18. *Id.* at 222. Further, because of the extent to which electronic mail (e-mail) has become such a commonplace term, it is worth noting that before full internet access was publicly available, BBS technology limited e-mail exchange to the users of a particular BBS and could not send e-mail between two different BBSs. *Id.* at 219 n.10.

19. Computer users may use shareware software without paying any sort of fee to the creator of the program. *See* Specht v. Netscape Communs. Corp., 306 F.3d 17, 24 (2d Cir. 2002) (noting that shareware websites contain "free, publicly available software"). For many shareware programs, the sole means of distribution was through legitimate computer BBSs (now websites). *Id.*

20. Jensen, s*upra* note 16, at 221.

21. *See id.* (stating that passwords were needed for full access to the board).

22. The NUP was never guessable and would change periodically; a user would often have to obtain the NUP directly from a current member of the BBS. *See* Aphex Twin, *How 2 Become And* [sic] *Elite Warez Trader*, LOW SELF ESTEEM (July 2, 1996), *at* http://web.textfiles.com/ezines/LSE/lse-11.txt (describing the process, including New User Voting, to become a member of the computer underground "elite").

23. *Id.*

24. For example, NUV frequently required a new user to explain the acronym H/P. H/P did not stand for Hewlett Packard, but for Hacking/Phreaking. *Id.* A more difficult test may have asked a user to define h/p/c/a/v: hacking/phreaking/carding/anarchy/virus. *Id.* Even further, many questions

that was still not a guarantee of admission—after the NUP was the requirement of New User Voting ("NUV"). The NUV system presented the new candidate's answers to the current members of the BBS, who would then vote to grant or decline admission to the candidate.[25] If the members balloted favorably, the final say on admission then rested with the sysop.[26]

Such rigorous standards ensured that those unwelcome never entered. It was an effective scheme. Law enforcement could not simply dial into a BBS and gain access. If a law enforcement officer desired access, it would be necessary to establish a reputation in the computer underground over months or years, learn the technical jargon, have personal references, and then pass the NUV process.[27] In addition, even if one did gain access, there were certain established principles that would alert users of a BBS to the presence of an outsider or law enforcement official. For instance, it was common practice to replace all instances of the letter "f" with its phonetic equivalent, "ph." Conversely, "f" often replaced "ph."[28] There were also well-known maxims, such as "Never trust anyone who types in all caps" or "Never trust anyone who abbreviates with' as 'w/."[29]

Considering the selective nature of the application process and the resultant privacy of communications within an exclusive BBS, it is no wonder that hackers commonly used BBSs as tools for organized fraud.[30] While speaking about crime in the abstract was obviously not illegal, hackers engaged in more than casual conversation and often directly conspired to engage in illegal conduct.[31] Unquestionably illegal and found within many BBSs, were illicit communications with no legitimate legal purposes.[32] Such communications often consisted of stolen calling card information, telephone company access numbers, or credit card

---

asked the candidate which BBSs he was currently a member of and for personal references connected to the computer underground. *Id*.

25. *Id.*

26. The final say of the sysop was not by some form of autocratic design, but rather only a product of the technical limitations of a computer BBS. Because the BBS resided entirely within the computer of the sysop, the sysop of course had complete power over which users had access. *See* Jensen, *supra* note 16, at 219 (stating that "[t]he operator has ultimate . . . control over this conduit").

27. Twin, *supra* note 22.

28. For instance the sentence "My telephone was fingered by the police," would read "My telefone was phingered by the police." For a more-than-adequate example of hacker spellings, see any Cult of the Dead Cow (computer hacker group) textfile newsletter, *at* http://www.textfiles.com/100/cDc-0200.txt (last visited May 14, 2005).

29. *Id.* After three years of legal education, it is probably worth noting that the constant use of abbreviation may be an indicator of a legal education, a good tip-off that someone does not belong on the BBS.

30. STERLING, *supra* note 8, at 154.

31. *Id.*

32. *Id.*

information.[33] Although it was not entirely uncommon for hackers to post such data publicly,[34] most data of this sort was sent by way of electronic mail between users.[35] Because Operation Sundevil sought to stamp out telephone and credit card abuse, it is not surprising that the investigation focused primarily on BBSs.[36]

Aside from being the digital nerve center for the trading of illicit access codes and encouraging the theft of services and fraud, law enforcement targeted BBSs for another compelling reason: evidence.[37] Seizing a computer hard drive that contained an entire BBS yielded a virtual cornucopia of evidence.[38] Law enforcement seizure of a BBS accomplished the digital equivalent of tapping phones and intercepting mail, and obviated all those pesky due process and Fourth Amendment concerns associated with actual phone taps and mail intercepts.[39]

In 1992 there were approximately 30,000 operational BBSs in the United States.[40] Operation Sundevil effectively seized twenty-five BBSs, or one tenth of one percent of all BBSs in the United States.[41] As Bruce Sterling notes, "[s]een objectively, this is something less than a comprehensive assault."[42] Nonetheless, it was an effective operation on various levels.

Chiefly, law enforcement found the copious amount of evidence on a BBS very useful.[43] Much information stored on a BBS gave law enforcement an indication as to how hackers and phone phreaks prevented

---

33. Jensen, *supra* note 16, at 230.

34. The underground elite eschewed this practice because such access codes would become widely known to many hackers or phone phreaks and consequently the telephone company or credit card company would terminate the code shortly after its publication. *See* AT&T Takes New Steps to Stop Calling Card Fraud (July 9, 1993) [hereinafter AT&T Memo] (distributing an AT&T internal memorandum dated July 9, 1993 which detailed the implementation of the Computerlinked Matching and Reporting Fraud Detection System whereby AT&T computers would attempt to find a match between all calling cards in use to determine if more than one person was using the same calling card simultaneously), *at* http://www.textfiles.com/phreak/at&t-cmr.txt. Use of such an access code could then tip-off law enforcement to investigate the user for further fraud. *Id.*

35. *See supra* text accompanying note 18.

36. *See supra* text accompanying note 13.

37. STERLING, *supra* note 8, at 155.

38. *Id.* Sterling writes that "[a]ll that busy trading of electronic mail, all those hacker boasts, brags, and struts, even the stolen codes and cards, can be neat, electronic, real-time recordings of criminal activity." *Id.*

39. *See id*. (stating that seizing a board is "as effective as tapping phones or intercepting mail").

40. *Id.* at 156.

41. *Id.*

42. *Id.*

43. *See* Guest v. Leis, 255 F.3d 325, 334 (6th Cir. 2001) (discussing the abundant amount of evidence available on a hard drive containing a BBS).

their exploits from being traceable.[44] This information afforded law enforcement the opportunity to get ahead of the curve in terms of curtailing and prosecuting wire fraud.[45] Further, by seizing computer equipment Operation Sundevil effectively muted the sysops of BBSs, who were often some of the most egregious offenders.[46]

Operation Sundevil accomplished these surface-level objectives quite well. The large amount of publicity noticeably slowed the illicit trafficking of credit and calling card information (although far from effectively halted).[47] However, mysteriously absent from Operation Sundevil were what one would normally expect to follow any major search and seizure operation: arrests.[48]

The overarching purpose of Operation Sundevil, then, was not to imprison offenders. As Bruce Sterling aptly notes, "Sundevil's motives can only be described as political."[49] Sterling further states, "[i]t was a public relations effort, meant to pass certain messages, meant to make certain situations clear: both in the mind of the general public and in the minds of various constituencies of the electronic community."[50] In other words, Operation Sundevil was a public relations stunt of old technique in a new context.[51]

Arguably, Operation Sundevil was a brilliant strategy. Even the most optimistic law enforcement agency could not hope to entirely halt the burgeoning underground trade and exploitation of telephone and credit card information.[52] By not arresting any sysop in connection with the seizure of computer equipment and subsequent mining of evidence, law enforcement did not implicate any of the constitutional concerns traditionally associated with arrests, such as probable cause and habeas corpus.[53] Furthermore, on the evidence seized was an incredible amount of incriminating material, so

---

44. STERLING, *supra* note 8, at 156–57.

45. *Id*. Bruce Sterling further writes that "[b]oards . . . full of brags and boasts, codes and cards, offer evidence in the handy congealed form." *Id.* at 157.

46. *Id.*

47. *Id.*

48. *Id*. at 157–58. Only four arrests occurred as a result of Operation Sundevil, and those arrests were not related to computer hacking or phone phreaking but resulted from possession of either illegal firearms or narcotics. *Id.* However, law enforcement seized 23,000 floppy disks which contained a plethora of both legal and illegal materials. *Id*. at 159.

49. *Id*. at 161.

50. *Id.*

51. *Id.* at 162.

52. *See* AT&T Memo, *supra* note 34 (discussing the widespread problem of calling card fraud).

53. *See Guest*, 255 F.3d at 342 (holding that the Ohio Regional Electronic Computer Intelligence Task Force did not violate plaintiffs' rights when it seized computer systems in connection with a BBS obscenity case).

much that no adversely affected party would dare ask for the seized materials back.[54] This information gave law enforcement an advantage over the sysops of BBSs.[55] Law enforcement could demand the sysops' cooperation in subsequent investigations by threatening prosecution for their failure to fully comply.[56] Another successful aspect of Operation Sundevil was the media attention. The media attention that the investigation attracted reassured the public that law enforcement was looking after their interests.[57] Most importantly, Operation Sundevil functioned effectively as a deterrent by sending a direct message to the computer underground that law enforcement was now on the beat and actively patrolling in cyberspace.[58]

In sum, Operation Sundevil portended what was to come should the computer underground continue its brazen disregard for the criminal laws. After Operation Sundevil became national news, states began to enact legislation beyond the fraud-related interests of Operation Sundevil in order to deal expressly with computer-related crimes, and such legislation came in very diverse forms.

II. THE MODERN APPROACHES TO PROSECUTING CYBERCRIME

It is not surprising that every state has now enacted some form of statute enabling the prosecution of cybercrimes.[59] It should also not be surprising that the ways in which the various states have approached the proscription of cybercrimes and their prosecution are as diverse as the states themselves. A survey of the nation's response to computer crime reveals a myriad of approaches and statutes directed towards preventing and responding to cybercrimes.[60] This Note focuses on the most popular and

---

54. STERLING, *supra* note 8, at 162. *But see* Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 438 (W.D. Tex. 1993) (holding that the U.S. Secret Service proximately caused lost sale damages in the amount of $100,617 when they seized the work product and equipment of a publisher in connection with a BBS raid).

55. STERLING, *supra* note 8, at 162.

56. *See id*. (noting that the police can use the seized evidence to put pressure on the sysops).

57. *Id.* at 165.

58. *Id*. at 162. Sterling descriptively asserts that Operation Sundevil sought to prove that law enforcement "were on the watch everywhere, even in those sleazy and secretive dens of cybernetic vice, the underground boards." *Id.*

59. It is worth mentioning that Vermont was the final holdout. But in 1999, Vermont enacted comprehensive legislation directed at cyber crimes by passing Chapter 87, Computer Crimes, VT. STAT. ANN. tit. 13, §§ 4101–4107 (Supp. 2004). *See* Julie A. Tower, Note, *Hacking Vermont's Computer Crimes Statute*, 25 VT. L. REV. 945, 945 (2001) (providing an in-depth analysis of Vermont's computer crime statute and describing the events that led to its adoption).

60. The approaches and statutes run the gamut, proscribing general acts such as unlawful use of a computer to the very specific proscription of unlawful use of computer encryption technology. *See*

relevant forms of computer crime statutes: Computer Fraud,[61] Unauthorized Use of a Computer and Computer Trespass,[62] and Interruption of Computer Services.[63]

A. Computer Fraud

Operation Sundevil intended to send a clear message to those engaging in various types of telephone and credit fraud.[64] In the early 1990s this was one of the most pressing concerns of law enforcement.[65] Before the ubiquitous proliferation of the Internet, before Grandma had an e-mail address, when cyberspace was still only a word used in science fiction novels, neither the federal government nor law enforcement were in the business of protecting the nation from a cyberattack.[66] Certainly, the sensationalism of computer hackers was alluring to Hollywood, but to the mind of the average American, the stories were purely fictional.[67] It is no wonder, then, that Operation Sundevil's intent was putting an end to fraud. Fraud, after all, was something that the ordinary citizen could relate to, something that was not difficult for law enforcement officers to analogize, many of whom had never operated, let alone owned, a computer. Probably because of the ease with which law enforcement and politicians could analogize fraud to common real space crimes, stamping out electronic fraud was the beginning, a precursor of sorts, to the modern approaches of prosecuting cybercrimes of more pressing national concern.

The problem, however, did not end with Operation Sundevil. In fact there was a rapidly growing state interest in curtailing computer-related fraud. Today, eight states have statutes that relate directly to computer fraud, many of which are entitled "computer fraud."[68] However, some

---

discussion *infra* Part II.A.

61. *Infra* Part II.A.

62. *Infra* Part II.B.

63. *Infra* Part II.C.

64. *See supra* text accompanying notes 49–50.

65. *See supra* text accompanying note 11.

66. The first use of the word 'cyberspace' is unknown, although the concept was no doubt embodied in the science fiction novels of William Gibson. *See generally* WILLIAM GIBSON, NEUROMANCER 4–5 (1984) (presenting a futuristic world in which exists an alternative reality akin to cyberspace).

67. *See* WARGAMES (MGM / UA Studios 1983) (detailing the story of a teenage computer hacker who inadvertently comes close to starting the third World War).

68. Eight states have computer fraud statutes: Arkansas, Hawaii, Illinois, Louisiana, Mississippi, North Dakota, Virginia, and West Virginia. ARK. CODE. ANN. § 5-41-103 (Michie 1997); HAW. REV. STAT. § 708-891 (1993); 720 ILL. COMP. STAT. ANN. 5/16D-5 (West 2003); LA. REV. STAT. ANN. § 14:73.5 (West 1999 & Supp. 2004); MISS. CODE ANN. § 97-45-3 (2000 & Supp. 2004); N.D. CENT. CODE § 12.1-06.1-08 (1997 & Supp. 2003); VA. CODE ANN § 18.2-152.3 (Michie 1996); W. VA.

statutes generally proscribe fraudulent activity, electronic or not, with theft of services statutes.

While theft-of-services statutes still apply to general phone fraud,[69] computer fraud statutes target crimes in which one uses a computer to perpetrate the fraud.[70] Virginia's computer fraud statute is a good model of many of the common elements found in computer fraud statutes. The statute reads, "Any person who uses a computer or computer network without authority and with the intent to: 1. Obtain property or services by false pretenses; 2. Embezzle or commit larceny; or 3. Convert the property of another shall be guilty of the crime of computer fraud."[71] Under Virginia's computer fraud statute, when the damages of the fraud rise, so does the punishment.[72] As noted, while theft of long distance services by the use of stolen credit or calling cards might be the subject of criminal charges based on existing theft of services provisions of the law, many states found it desirable to enact statutes that dealt directly with computer-related crime.[73] Computer fraud statutes thus operate on the assumption, erroneous or not, that crimes involving computers are somehow more dangerous or may be more injurious to the victims and society. That is, because of society's ever-increasing reliance on computers and technology, attacks targeting important computer systems have the potential to seriously

---

CODE ANN. § 61-3C-4 (Michie 2000). It is worth noting that thirteen states have codified laws that directly relate to the theft of computer services: Delaware, Georgia, Massachusetts, Minnesota, Montana, Nebraska, Nevada, New Hampshire, Oregon, Pennsylvania, Texas, Virginia, West Virginia. DEL. CODE ANN. tit. 11, § 933 (2001); GA. CODE ANN. § 16-9-93(a) (2003); MASS. GEN. LAWS ch. 266, § 33A (2002); MINN. STAT. ANN. § 609.893 (West 2003 & Supp. 2004); MONT. CODE ANN. § 45-6-307 (2004); NEB. REV. STAT. § 28-1344 (1995); NEV. REV. STAT. ANN. 205.4765 (Michie 2003); N.H. REV. STAT. ANN. § 638:17(II) (1996 & Supp. 2003); OR. REV. STAT. § 164.125 (2003); 18 PA. CONS. STAT. ANN. § 3926 (West 1983 & Supp. 2004); TEX. PENAL CODE ANN. § 33.01 (Vernon 2003 & Supp. 2004); VA. CODE ANN. § 18.2-152.6 (Michie 1996); W. VA. CODE ANN. § 61-3C-5 (Michie 2000 & Supp. 2003).

69. For example, calling card theft and subsequent misuse thereof by way of low tech "shoulder surfing" techniques are still within the purview of theft-of-services statutes. *See* Jayson Blair, *Arrests Reveal New Way to Steal Phone Card Data*, N.Y. TIMES, July 4, 1998, at B1 (describing shoulder surfing as "glancing over the shoulders of callers and writing down their calling card numbers and security codes").

70. An up-to-date example of such fraud is auction/Internet fraud, in which an offender uses a computer in order to entice a victim with fraudulent solicitations through online auction websites or spam email opportunities. *See* United States v. Bell, No. 02-4944, 2003 U.S. App. LEXIS 15435, at *25–26 (4th Cir. Aug. 1, 2003) (per curiam) (detailing defendant's acts of selling close to 200 collectible sports cards on an Internet auction, obtaining payment, and then refusing to ship the items).

71. Computer Fraud, VA. CODE ANN. § 18.2-152.3 (Michie 1996).

72. *Id.* Where the value of the fraudulently obtained property or services is over $200, the crime is punishable as a Class 5 felony; where the value is less than $200, the crime is punishable as a Class 1 misdemeanor. *Id*.

73. *See, e.g.*, ARK. CODE ANN. § 5-41-101 (Michie 1997) (detailing the legislative intent of Arkansas' codification of specific provisions dealing with computer-related crimes).

damage the nation's infrastructure. Therefore it follows that it is wise that specific statutes target computer-related criminal activity,[74] and that their penalties be harsher than their mundane real-space counterparts.[75]

It is important to recall that while Operation Sundevil's intent was to curb credit card and calling card fraud, as well as other methods of obtaining long distance telephone calls without pay, law enforcement specifically targeted the computer underground.[76] BBSs, as previously noted, were the primary means of communication for the underground elite.[77] Only calling BBSs within a local calling area and thus obviating the need for long distance calls, could hardly prove a user as part of the underground elite.[78] Rather, an aspirant to the ranks of the underground elite quickly realized that BBSs that were part of the upper echelon of the computer underground were often located around the United States and the globe.[79] Unless a user had tremendous amounts of money to spend on long distance charges, a user could not be part of the underground elite without a firm grasp of how to defraud the telephone company.[80] Generally, computer hackers exploited calling cards or PBXs by using elaborately written scripts to dial into a particular telephone system[81] and input stolen access codes at the appropriate times.[82] Ultimately the script would connect the modems of the computer hacker and the BBS together, all the while charging the middle man (PBX owner) for the long distance charges of the telephone call.[83]

Considering the myriad of ways in which an offender could use a computer to commit fraud, computer fraud statutes have to be very broad

---

74. *Id*.

75. *See, e.g.*, LA. REV. STAT. ANN. § 14:73.5 (West 1999 & Supp. 2004) (stating that the crime of computer fraud shall be punishable by imprisonment with or without hard labor for up to five years); W. VA. CODE ANN. § 61-3C-4 (Michie 2003) (punishing computer fraud with up to ten years imprisonment).

76. *See supra* text accompanying notes 11–13.

77. *See supra* text accompanying notes 19–22.

78. *See* Twin, *supra* note 22 (describing the process of becoming an elite member of the underground warez trafficking scene).

79. *Id.*

80. *Id.*

81. Such scripts precisely timed the moments when the telephone system required an access code and then input the code at the precise time.

82. PBX stands for Private Branch Exchange; generally, a PBX is an outside entrance into an internal phone system, usually requiring knowledge of an access code. Once within a PBX system, depending upon the features of the PBX, a user could frequently place long distance calls billed to the company operating the PBX. *See* Isaac Hillson, *Thwarting the PBX Hacker*, NETWORK MAGAZINE (Sept. 5, 2002) (describing methods businesses can use to protect their PBX systems from hackers), *available at* http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleID=7619284.

83. *Id.*

indeed. They must also be broad enough to encompass another favorite pastime of the computer underground: software or "warez" trafficking.[84] As the speed of modems increased, so too did the ability to transfer larger files between computers.[85] Warez trading became an integral part of the computer underground.[86] Warez trading sparked the creation of entire BBSs whose sole purpose was to traffic pirated software.[87] Warez traders formed underground groups, colloquially known as courier groups, whose members consisted of individuals with fast modems, access to "codes," programming experience, and cryptoanalytic backgrounds.[88] The perquisite was that being a warez courier for an elite warez courier group often guaranteed one access to the most elite BBSs.[89] However, first someone had to somehow pirate the software, or "crack" as the term was often used, before another member would courier it to any number of BBSs.[90] Therefore, with the intent of filling the very sought after niche of cracking software quickly, skilled programmers who prided themselves on quickly and consistently being able to crack software encryption techniques formed their own underground groups.[91] As a result of the combined efficiency of couriers and cracking groups, shortly after a software company released a new product, it found its way to BBSs all over the country and world.[92] Computer fraud statutes thus brought within their purview the trafficking and pirating of software.[93]

While prosecutors could employ computer fraud statutes to prosecute members of the computer underground who used codes to make free long-distance phone calls as well as warez couriers, the punishments were,

---

84. "Warez" is the computer underground term for "software." *See* Twin, *supra* note 22 (describing how to become a warez trader).

85. By 1991, modem speeds had increased from 2,400 bits per second (BPS) to 14,400 BPS; one megabyte of data on a 2,400 BPS modem took over one hour to transfer; a 14,400 BPS modem could transfer one megabyte of data in approximately ten minutes. *See Introduction and History of Modems*, *at* http://www.dementia.org/~julied/tele2100/intro.html (last visited July 29, 2005) (providing an introduction to and describing the evolution of modem-based computer communications).

86. *See* Twin, *supra* note 22 (describing the importance of the warez scene).

87. *Id.*

88. "Codes" is shorthand for any type of access code whereby one could obviate long distance charges. For example, credit card numbers, calling card numbers or PBX access numbers are all codes.

89. *See* Twin, *supra* note 22 (describing the warez scene).

90. *Id.*

91. *Id.*

92. *See* STERLING, *supra* note 8 at 159 (summarizing Sundevil's acquisition of approximately 23,000 floppy disks of data, including pirated games and stolen codes).

93. The participle "pirating" is being used in the sense of the overall scheme of stealing software, not in the technical sense of breaking encryption schemes which software companies intended to prevent piracy. The Digital Millennium Copyright Act of 1998, 17 U.S.C. § 1201 (2000), encompasses actual piracy and intended, ostensibly, to prevent the piracy of the film and recording industry's intellectual property by criminalizing the circumvention of any digital encryption technology.

because of the strict guidelines the statute imposed, arguably disproportionate to the offenses they sought to deter.[94] The threshold amount of services or property obtained to prosecute an offense as a felony was often low and easily met.[95] Engaging in only a single fraudulently made telephone call or trafficking a single piece of pirated software was enough to prosecute the offense as a felony.[96] As a pressure device, computer fraud statutes are very effective. A fifteen-year-old charged with multiple felonies, facing jail time, and under tremendous pressure, oftentimes will proverbially "spill the beans." Thus computer fraud statutes continued one of the main functions of Operation Sundevil: obtaining evidence. These statutes were an effective way to obtain evidence, mostly in the form of leads and testimony, pertaining to the larger schemes of a courier group.[97]

The breadth of computer fraud statutes in proscribing computer-based-fraud schemes were most certainly a response to various frauds perpetrated through the Internet. Indeed, frauds perpetrated through the Internet have become so prevalent that the FBI and the National White Collar Crime Center (NW3C) jointly created the Internet Fraud Complaint Center (IFCC) website, which is dedicated solely to allowing victims of Internet fraud to report schemes directly to the FBI and NW3C.[98] During 2002 alone, the IFCC website received 75,063 complaints regarding a plethora of online frauds, including, but not limited to: "auction fraud, credit/debit card fraud, computer intrusions, unsolicited email (SPAM), and child pornography."[99] Perpetrators primarily resided in the following states: California, New York, Florida, Texas, and Illinois.[100] The monetary loss from Internet fraud rose from $17 million in 2001 to over $54 million in 2002.[101] The average loss per complaint to the IFCC was $299.[102] There was not a strong correlation between age and loss, but the proportion of victims over sixty

94. *But see supra* text accompanying note 48 (noting that arrests are rare).

95. *See* Computer Fraud, VA. CODE ANN. § 18.2-152.3 (Michie 1996) (stating that offenses involving over two hundred dollars or more shall be punished as a felony).

96. *Id.*

97. It is worth noting that often the machinations of courier groups or computer hacker groups generally, provided that sufficient evidence of their collaborative activity was obtained, were also brought within the purview of the Racketeer Influenced Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961–1968 (2000).

98. Internet Fraud Complaint Center, *at* http://www.ifccfbi.gov (last visited July 28, 2005).

99. IFCC 2002 INTERNET FRAUD REPORT, January 1, 2002—December 31, 2002 at 3, *available at* http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf (last visited July 28, 2005).

100. *Id.* Interestingly, of this list, only Illinois has passed a specific computer fraud statute. *See* Computer Fraud, 720 ILL. COMP. STAT. ANN. 5/16D-5 (West 2003).

101. IFCC 2002 INTERNET FRAUD REPORT, *supra* note 99.

102. *Id.*

years old who lost more than $5,000 was significantly higher than any other age category.[103] The cost of each instance of fraud the IFCC detailed was sufficient to punish each offense as a felony.[104] Considering the extent of the monetary damages, the negative effect on state commerce, and the targeted victims, there was a very compelling state interest in curbing further Internet fraud.

Broadly defined, computer fraud may encompass many fraudulent activities performed on the Internet. As a deterrent, computer fraud statutes mete out an appropriately harsh penalty. However, when compared with the computer fraud of members of the computer underground, it hardly seems equitable to punish Internet fraud and the fraud of the computer underground under the same statute. For the former are traditional crimes, such as confidence scams, that prey upon the insecurities of the elderly and the general population's inherent lack of technological understanding, and the latter are merely taking advantage of telephone company insecurities. Fraud that targets the elderly has an immediate and direct effect on the quality of elderly persons' lives. However, fraud that targets telephone company insecurities is arguably victimless, and does not deteriorate the quality of a victim's life. Nonetheless, protecting the proliferation of commerce through the Internet is a laudable state interest. Therefore, in the interest of equity and proportionality of punishment, computer fraud statutes should cover a broad range of fraudulent activities, but with the scope limited to perpetuating frauds by way of the Internet. The law should prosecute traditional fraud, as in theft of long distance services, in the traditional sense, and carry with it a less severe punishment than the injurious offenses of confidence men preying upon the elderly.

B. Unauthorized Use of a Computer and Computer Trespass

"Unauthorized use of a computer" and "computer trespass" are very popular forms of cybercrime statutes; twelve states have enacted legislation addressing such action.[105] Unauthorized access and computer trespass are not difficult concepts to understand. Moreover, it is objectively and

---

103. *Id.*

104. *Id.*

105. Delaware, Hawaii, Iowa, Kentucky, Maryland, Massachusetts, Minnesota, Montana, Nebraska, Nevada, New Mexico, New York. DEL. CODE ANN. tit. 11, § 932 (2001); HAW. REV. STAT. § 708-895.5 (Supp. 2003); IOWA CODE ANN. § 716.6B (West Supp. 2004); KY. REV. STAT. ANN. § 434.845 (Michie Supp. 2003); MD. CODE ANN., CRIM. LAW § 7-302 (2002); MASS. GEN. LAWS ch. 266, § 120F (2002); MINN. STAT. ANN. § 609.891 (West 2003); MONT. CODE ANN. § 45-6-311 (2004); NEB. REV. STAT. § 28-1343.01 (1995); NEV. REV. STAT. ANN. 205.4765(3) (Michie 2001); N.M. STAT. ANN. § 30-45-5 (Michie 2004); N.Y. PENAL LAW § 156.05 (McKinney 1998).

morally wrong to use something without permission or to trespass on property when there is no right to enter. It is easy to analogize these crimes to familiar offenses, and that may be partly responsible for the quantity of these statutes.[106]

On the forefront of the prevention of computer crime is New York. However, New York is atypical because it treats the offenses of unauthorized use and computer trespass entirely differently. "Unauthorized use of a computer" is limited to the following situation:

> A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.[107]

"Computer trespass," on the other hand, reads as follows:

> A person is guilty of computer trespass when he knowingly uses or causes to be used a computer or computer service without authorization and:
> 1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or
> 2. he thereby knowingly gains access to computer material.[108]

New York's unauthorized-use-of-a-computer statute facially appears intended to prosecute those who knowingly access computer systems for the purpose of using such systems in an unauthorized manner.[109] It is the computer analogue of the crime of theft of services. On the other hand, New York's computer trespass statute targets those who, without authorization, access a computer or computer system.[110]

Legislators probably directed computer trespass statutes more towards computer hackers.[111] An offender needs only the intent to use the accessed computer system to commit or aid in the commission of a felony, or have

---

106. *See* Douglas Thomas, *Criminality on the Electronic Frontier*, *in* CYBERCRIME 21 (Douglas Thomas & Brian D. Loader eds. 2000) (stating that one of the primary problems law enforcement faces with cybercrimes is the difficulty of linking cybercrimes with the real world).

107. N.Y. PENAL LAW § 156.05 (McKinney 1998).

108. § 156.10.

109. § 156.05.

110. § 156.10.

111. *See id.*

actually accessed computer material without authorization.[112] However, New York's statutory language for the crime of unauthorized use of a computer necessarily implies that an offender also be guilty of computer trespass.[113] The obverse is also true: because a primary element of computer trespass is "use" of a computer, there can be no guilt of computer trespass without unauthorized use of a computer.[114] By the overlapping statutory language, prosecutors may bootstrap additional charges against a defendant and consequently stack additional penalties and jail time.

Consider the case of *People v. Esposito*, which is particularly illustrative of such bootstrapping.[115] In *People v. Esposito*, prosecutors charged the former police chief of a commuter railroad with unauthorized computer use and computer trespass for allegedly using a State Police computer system to access the criminal history of an individual without an authorized criminal justice purpose.[116] While the court ultimately dismissed the indictment on grounds unrelated to the statutes at issue, it demonstrated that one offense necessarily overlaps with the other.[117]

Massachusetts, on the other hand, has taken a more sensible, and arguably more equitable approach, by combining the two offenses into one statute: "Unauthorized access to computer system."[118] The Massachusetts statute defines an offender as, "[w]hoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access . . . ."[119] Here, the focus is not on the means by which an intruder obtains access but entirely upon the *access* itself of a computer or computer system with knowledge that doing so is without authorization.[120] In this sense, one need not actually use a computer without authorization; access without authorization is sufficient for the statute to operate. This is not to say that Massachusetts has no law respecting unauthorized use of computers. Indeed, Massachusetts does have its own statute proscribing unauthorized use; however, the statute is

---

112. *Id.*

113. § 156.05.

114. *Id*.

115. People v. Esposito, 553 N.Y.S.2d 612, 613 (N.Y. Sup. Ct. 1990).

116. *Id.* at 613.

117. Prosecutors ultimately dismissed the charges against Esposito because the indictment was obtained by New York City Special Prosecutors authorized by N.Y. COMP. CODES R. & REGS. tit. 9, section 1.55 (2004) to prosecute only "corrupt" acts arising out of law enforcement. Because Esposito did not receive any personal benefit, his actions were not "corrupt." *Esposito*, 553 N.Y.S.2d at 616.

118. MASS. GEN. LAWS ch. 266, § 120F (2002).

119. *Id.*

120. *Id.*

very narrow and specifically targets the unauthorized access of subscription-based computer systems.[121]

While not restricted to prohibiting the unauthorized use of subscription-based systems, New Mexico's approach to the problem of unauthorized use of and access to computer systems is perhaps the most sensible and equitable. It is at once broad enough to encompass many types of computer-related offenses relating to unauthorized access and narrow enough to prevent bootstrapping and disproportionate results.[122] New Mexico's unauthorized-computer-use statute requires that a person "knowingly . . . and without authorization, or having obtained authorization, uses the opportunity such authorization provides for purposes to which the authorization does not extend . . . ."[123] The statute is broad enough to encompass unauthorized access to commercial computer systems, much like Massachusetts's statute directed specifically towards such access, as well as computer trespass offenses.[124] Notably, computer trespass itself is not sufficient to invoke the statute because the focus is on the use of a computer system.[125] Accordingly, the statute punishes unauthorized use along specifically delineated lines of damages.[126] Penalties range from a petty misdemeanor for damages of one hundred dollars or less to a second-degree felony for damages exceeding twenty thousand dollars.[127]

This is also the manner in which Kentucky, Minnesota, and Montana delineated penalties for their unauthorized-use statutes.[128] Nevada's system similarly delineates penalties proportionate to the offense but along differing lines.[129] Nebraska's statute prioritizes general computer trespass offenses that merely compromise the security of a computer system, without more, as the least punishable offense.[130] That is, Nebraska's statute

---

121. *See* Obtaining Computer Services by Fraud or Misrepresentation, MASS. GEN. LAWS ch. 266, § 33A (2002) (focusing on the unauthorized access of commercial computer systems).

122. *See* N.Y. PENAL LAW §§ 156.05–156.10 (McKinney 1998) (allowing the prosecution to bootstrap a defendant with charges of unauthorized use and computer trespass even though the elements of each offense are basically identical); *see also supra* text accompanying notes 112–17.

123. N.M. STAT. ANN. § 30-45-5 (Michie 2004).

124. MASS. GEN. LAWS ch. 266, § 33A (2002).

125. N.M. STAT. ANN. § 30-45-5.

126. *Id.*

127. However, unlike New York or Massachusetts, New Mexico's approach to unauthorized use encompasses the access and use of a computer or computer system and actions of copying, obtaining possessing, concealing, or copying any computer or computer system. *Id.* Because of the statutory proscription focusing on actions and broadly defining the objects of the proscribed actions, the unauthorized-use statute undoubtedly was intended to also combat computer piracy.

128. KY. REV. STAT. ANN. §§ 434.845-434.855 (Michie Supp. 2003); MINN. STAT. ANN. § 609.891 (West 2003); MONT. CODE ANN. § 45-6-311 (2004).

129. NEV. REV. STAT. ANN. 205.4765 (Michie 2001 & Supp. 2003).

130. NEB. REV. STAT. § 28-1343.01 (1995).

emphasizes the nature of the risk that unauthorized access poses to persons and the public.[131] Nevada took a similar approach for unauthorized access, providing that by itself it is merely a misdemeanor offense.[132]

Unauthorized use of a computer system and computer trespass are similar offenses, and states have treated them similarly.[133] Their elements, however, should not overlap. Undoubtedly, law enforcement and industry should not countenance computer trespassers without penalty. Yet, the law should not treat a computer trespass alone as a grievous offense without the trespass causing actual damages that stem from an unauthorized use of a computer system in the form of theft of services or the acquisition of private information. The difference is one of intent; namely, exploration versus personal benefit, and the law should treat the latter more severely. Nonetheless, because computer trespass and unauthorized use pose significant dangers, the most sensible method of punishment is Nebraska's approach of assessing the danger that a particular computer intrusion causes.[134] Only serious consideration of the dangers that trespass and unauthorized use pose will enable the law to treat trivial and grievous offenses equitably and proportionately.

C. Interruption of Computer Services

While individual computer intrusions may be troublesome and a nuisance for government agencies and companies, the threat to a network's infrastructure from mere intrusion is slight, unless the intruder has the malicious intent to disrupt network services. However, offenders usually accomplish a disruption of computer services from without a network by using Denial of Service (DoS) attacks or a Distributed Denial of Service (DDoS) attacks.[135] DoS attacks are for the most part self-explanatory, in the sense that they deny users of a network the resources normally available.[136] The most common methods of DoS and DDoS attacks take the form of undue bandwidth consumption, computer resource theft, exploitation of flawed programming, and traffic redirection.[137] To carry out

131. *Id.*

132. NEV. REV. STAT. ANN. 205.4765 (Michie 2001 & Supp. 2003).

133. *See supra* text accompanying notes 121–24.

134. NEB. REV. STAT. § 28-1343.01 (1995).

135. *See* Bland_inquistor, *Denial of Service Attacks, Tools of the Tools*, 2600 THE HACKER QUARTERLY, Fall 2003, at 41 (describing DoS and DDos attacks).

136. *Id.* at 40.

137. *Id.* at 40–41.

such attacks, one need not be a technical wizard as there are easy-to-use programs which facilitate DoS and DDoS attacks.[138]

It is worth noting that this analysis does not imply that any attempt to disrupt computer services deserves the utmost punishment. Rather, some disruption, while seriously affecting some companies or institutions, is not by any means a national threat. For instance, the first of the long theorized DDoS attacks came in February of 2000 and affected, most notably, eBay, Amazon.com, and CNN.com, as well as five other major commercial networks.[139] A now infamous adolescent computer hacker who went by the handle of "Mafiaboy" used commonly available techniques to completely disrupt network operations.[140] While Mafiaboy aimed his DDoS attack at major websites to protest the commercialization of the Internet, his actions were not a national security threat. For many users it must have been an inconvenience to find that eBay, Amazon.com, or CNN.com was offline, but the nation's information infrastructure remained intact and in perfect working order. What was threatening, however, was that such an attack could be so easily orchestrated and effectuated.

With minimal effort and a modicum of skill an attacker could knock major websites offline and slow networks down to a halt.[141] Considering the ease with which an attacker could orchestrate a catastrophic DDoS attack, it would not be surprising if computer security professionals and legislators devoted substantial attention and effort towards preventing such an attack. Notwithstanding the highly publicized DDoS attacks of February 2000, only five states have statutes specifically directed towards the interruption of computer services.[142] Interruption of computer services statutes thus seek to proscribe conduct that intentionally or recklessly disrupts or degrades computer services or denies computer services to an authorized user.[143] Such statutes specifically intend to enable the prosecution of those responsible for DoS and DDoS attacks.[144]

---

138. *Id.* at 41 (referring to such attacks as "[c]anned DoS [a]ttacks").

139. *Id.*

140. Elizabeth Clark, *Lesson 182: Distributed Denial of Service Attacks*, NETWORK MAGAZINE, Sept., 2003, at 19.

141. Bland_inquisitor, *supra* note 135, at 40–41.

142. Delaware, Nebraska, Nevada, New Hampshire, West Virginia. DEL. CODE ANN. tit. 11 § 934 (2001); NEB. REV. STAT. § 28-1344 (1995); NEV. REV. STAT. ANN. 205.477 (Michie 2001); N.H. REV. STAT. ANN. § 638:17 (1996 & Supp. 2003); W. VA. CODE ANN. § 61-3C-8 (Michie 2000).

143. *See, e.g.*, Interruption of Computer Services, DEL. CODE ANN. tit. 11 § 934 (2001) (stating that the statute operates when a person "intentionally or recklessly disrupts or degrades" computer services).

144. *Id.*

DoS and DDoS attacks are undoubtedly becoming the most popular methods of cyberattack, chiefly because they are easy to orchestrate.[145] Mafiaboy was not the last to use DoS and DDoS attacks to make a statement. In fact, a loosely organized group, the "ElectroHippies," used DDoS attacks to shut down the World Economic Forum's (WEF) website during a meeting of the WEF in January 2002.[146] Similarly, repeated DDoS attacks allegedly forced out of business the British Internet service provider, Cloudnine.[147] There are also similar reports that DDoS attacks targeted Goldman Sachs and Investcorp.[148] Most interesting, however, are reports that Pakistan and India have employed DDoS attacks against each other.[149]

Mafiaboy, the ElectroHippies, and most likely, those responsible for DDoS attacks against Goldman Sachs and Investcorp were not intending to disrupt the information infrastructure of the entire United States.[150] Pakistan and India, however, utilized DDoS attacks in response to long-standing political and ideological conflicts between their two nations.[151] Yet, despite the difference between DDoS attacks that intended to convey a political message and DDoS attacks intended as a method of information warfare, interruption-of-computer-services statutes have treated both offenses identically.[152] Interruption-of-computer-services statutes allow for the prosecution of a political group that directs a DoS or DDoS attack against, for instance, a website that advocates Nazism, under the same statutes with and the same penalties as a group that launches a DDoS attack against a local medical clinic or a government-operated computer network.[153] While undoubtedly the law should punish such political activism as an act of civil disobedience, it does not make sense for the law

145. *See* Bland_inquisitor, *supra* note 135, at 41 (noting that "DDoS attacks require more forethought than DoS attacks, but that doesn't make them any harder to accomplish or any less common").

146. Jim Carr, *Good News/Bad News in DoS Struggle*, NETWORK MAGAZINE, July 1, 2002, at 32.

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.*

151. *See* Lawrence D. Casiraya, *UK Software Firm Expert Downplays Cyberterrorism*, BUSINESSWORLD, Jan. 10, 2003 (discussing a virus named "Yaha" of Indian origin which directed a DDoS attack against government websites in Pakistan).

152. *See, e.g.*, DEL. CODE ANN. tit. 11 § 934 (2001) (detailing the usual elements of interruption-of-computer-services statutes with the notable absence of any method to temper the severity of punishment according to an attacker's intent).

153. *See* discussion *infra* Part III (detailing recommendations for the more equitable prosecution of interruption of computer services offenses).

to regard such acts as tantamount to the danger of a DDoS attack that intentionally targets national-interest computer networks.[154]

Further, in addition to their failure to recognize that there may be different types of offenders, interruption of computer services statutes permit the prosecution of arguably innocent computer users who unknowingly facilitate DoS or DDoS attacks. That is, the language of interruption of computer services statutes also penalizes those who recklessly cause the disruption of computer services.[155] The most common method of implementing a DDoS attack is using an operating system security flaw to install a backdoor program that allows an attacker to remotely control a computer's operations.[156] With the proliferation of residential broadband Internet access that places home computers on a huge local area network, hundreds of thousands of home computer users are now vulnerable to operating system security flaws that may allow an attacker to infect their computers with backdoor programs facilitating remote access.[157] Generally, while updates are periodically available that attempt to patch particular security flaws and thereby prevent remote access, many users never install them.[158] Those users' computers become the "zombie" machines that actually launch DDoS attacks against a target, thus making it incredibly difficult for law enforcement to trace the origin of the attack.[159] While no court has addressed the issue, such users who are the owners of "zombie" machines and ignorant of the security implications of their inaction could arguably be subject to liability under interruption of services statutes for their reckless omission to properly secure their computer systems that are part of a local area network.[160]

It hardly seems fair to prosecute such innocent users. That is why legislators more likely intended the reckless element of the statute to permit the prosecution of virus and worm authors. In 2001, the Nimda worm became international news.[161] Nimda was a highly complex self-replicating

---

154. Many refer to Internet-related activism as "hacktivism." *See, e.g.*, sfear, *Introduction to Hacktivism* (Dec. 1999) (discussing the evolution and use of electronic protest), *at* http://www.collusion.org/Article.cfm?ID=109.

155. Interruption of Computer Services, DEL. CODE ANN. tit. 11 § 934 (2001).

156. *See* Bland_inquisitor, *supra* note 135, at 41 (describing placing "server" software on as many "zombies" as possible).

157. *Id.*

158. *See Microsoft: Committed To Homeland Security*, EWEEK, Jan. 14, 2004 (detailing an interview with Microsoft executives dealing, in part, with the security implications of the Windows patching system), *at* http://www.eweek.com/article2/0,4149,1436176,00.asp.

159. *Id.*

160. *See* Interruption of Computer Services, DEL. CODE ANN. tit. 11 § 934 (2001) (allowing the prosecution of a person who "recklessly" causes the interruption of computer services).

161. *E.g.*, Chen Bin, *Scourge of the Malicious Mobile Code*, THE BUSINESS TIMES SINGAPORE,

Internet worm that infected 2.5 million users and took just one day to propagate itself through the Internet.[162] Nimda grinded the servers that keep the Internet functioning not to a complete halt, but to a noticeably slower speed.[163]

Along with Nimda, other newsworthy Internet worms were Code Red and Blaster.[164] Even though Nimda, Code Red, and Blaster, first propagated themselves through the Internet two years ago and anti-virus manufacturers quickly developed countermeasures, they are still collectively responsible "for over 32,000 unique infected systems each day on the Internet."[165] The cost in bandwidth and loss of resources is probably so incredible that its exact cost is incalculable. Yet, analysts have assessed the total costs at well into the billions.[166]

Worms such as Nimda operate by exploiting Microsoft Windows vulnerabilities.[167] Because there is never a shortage of Windows security holes to exploit, and because construction of self-replicating worms is not an incredibly difficult task, any able and malevolent programmer may construct similar worms.[168] Therefore, it is entirely rational that interruption-of-computer-services statutes provide penalties for the reckless release of such worms. So long as the law does not penalize innocently ignorant computer users, interruption-of-computer-services statutes do have a legitimate basis for proscribing the reckless release of worms. Because only someone with the technical skill and knowledge to create a worm in the first place could cause the reckless release of a worm, it makes sense that the penalty is as harsh as the intentional release of a worm. In other words, the statute sends a clear message that the individual should have known better.

However, this was not always the case. In 1988, Robert Morris, Jr., then a graduate student studying computer science at Cornell, wrote an experimental self-replicating and propagating worm.[169] Morris

---

Dec. 31, 2001, at 16.

162. *2001: A Security-Odyssey; F-Secure Recalls the Most Challenging Year Ever for Data Security*, BUSINESS WIRE, Dec. 18, 2001.

163. *See id.*

164. *Arbor Networks Worm Researcher Jose Nazario Authors Groundbreaking Book on Worm Detection and Defense*, BUSINESS WIRE, Oct. 27, 2003.

165. *Id.*

166. George V. Hulme, *One-Stop Security Shop Doesn't Appeal To All*, INFORMATIONWEEK, June 16, 2003, at 26.

167. Brian Livingston, *Window Manager: Is It Secure? I Mean IIS*, INFOWORLD, Jan. 21, 2002, at 39.

168. *Id.*

169. *The Robert Morris Internet Worm*, *at* http://www.swiss.ai.mit.edu/6805/articles/morris-worm.html (last visited July 29, 2005) (providing a short overview of the *first* instance of an Internet

subsequently injected the worm into the Internet from a computer located at Massachusetts Institute of Technology (MIT).[170] Morris intentionally launched the worm from an MIT computer as a red herring intended to disguise the worm's origin.[171] Soon after the worm's release, Morris realized, much to his dismay, that the worm was replicating at a rate much faster than he had anticipated.[172] Even though there were not nearly as many computers and institutions connected to the Internet in 1988 as there are now, the worm had significantly affected universities, military sites, and medical research facilities.[173] The estimated damages at each affected site ranged from $200 to more than $53,000.[174] Federal prosecutors eventually convicted Morris for violating the Computer Fraud and Abuse Act,[175] and a judge sentenced him to three years of probation, 400 hours of community service, and fined him $10,050.[176]

Compare Morris's case with that of Jeffrey Parson. State authorities arrested Parson in August 2003 and charged him with writing and releasing a variant of the Blaster worm.[177] While the original Blaster worm infected approximately 500,000 computers worldwide, Parson's variant of the worm (Blaster-B) affected only 7,000 computers.[178] As with Morris, prosecutors charged Parson under the Federal Computer Fraud and Abuse Act.[179] However, if convicted, notwithstanding that Parson's culpability and effect on national interest computers was far less than that of Morris', Parson faces a $250,000 fine and up to ten years in prison.[180]

Interruption-of-computer-services statutes are well-intentioned and laudable attempts to criminalize conduct that is potentially dangerous.

---

worm).

170. *Id.*; *see also* KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER 220, 238 (1991) (providing an analysis of the Robert Morris Internet worm); *see generally* BRYAN CLOUGH & PAUL MUNGO, APPROACHING ZERO: DATA CRIME AND THE COMPUTER UNDERWORLD 98–105 (1992) (discussing the Robert Morris Internet worm along with the origin of the virus writing computer counter culture).

171. *The Robert Morris Internet Worm*, *supra* note 169.

172. *Id.*

173. *Id.*

174. *Id.*

175. 18 U.S.C. § 1030 (2000).

176. *The Robert Morris Internet Worm*, *supra* note 169.

177. George V. Hulme, *Legal Penalties: Hackers Face Longer Sentences*, INFORMATIONWEEK, Nov. 10, 2003 at 48, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=16000598.

178. Bob Evans, *Enterprise; View from the States; Get Tough with the Computer Saboteurs*, COMPUTING, Sept. 18, 2003, at 31.

179. *See* Hulme, *supra* note 177, at 48 (indicating that Parson was prosecuted under new sentencing guidelines).

180. Evans, *supra* note 178, at 31.

However, as this Note further explores in Part III, whether the law should treat civilly disobedient DoS attacks on websites as tantamount to DDoS attacks on networks of national and vital interest requires further consideration.[181] Similarly, while the reckless release of Internet worms is undoubtedly something the law should attempt to prevent, the issue of whether to impose criminal penalties for reckless and non-intentional release deserves more thought.

III. RECOMMENDATIONS FOR THE EQUITABLE PROSECUTION OF CYBERCRIME

Undoubtedly, it is wise for any state or nation to enact statutes hand-tailored specifically to prosecute cybercrimes. Some may claim that such statutes are merely old wine in new bottles. Some may claim that each cybercrime has an analogue offense already codified—that computer intrusion, for instance, is merely the digital equivalent of criminal trespass statutes. To facilitate the prosecution of cybercrime and deter it in the future, however, it is certainly advisable and laudable for state legislatures to construct statutes dealing explicitly and exclusively with cybercrime. Often, in states which have passed comprehensive computer crime statutes, the legislature's findings reflect these interests.[182] Because computer technology has become so pervasive, and because society's reliance thereon has become so entrenched, state legislatures have found that computer criminals have the opportunity to inflict substantial harm to the welfare of a state.[183] It logically follows, then, that the intent of such statutes and their primary aim should be to deter and punish such conduct when it occurs. However, while most cybercrime statutes allow for the prosecution of crimes that may affect the welfare of a state or other such lofty interests, they also punish to the same degree less culpable acts that, although certainly wrong and illegal, are not comparable in magnitude or intent.[184]

Computer fraud statutes, for example, ought to punish more harshly those who contribute to the degradation of commerce on the Internet and

---

181. *See supra* text accompanying note 154; *infra* Part III.

182. *E.g.* W. VA. CODE ANN. § 61-3C-2 (Michie 2000).

> While various forms of computer crime or abuse might possibly be the subject of criminal charges or civil suit based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which specifically proscribes various forms of computer crime and abuse and provides criminal penalties and civil remedies therefor.

Id.

183. *Id.*

184. *See* discussion *supra* Part II.C (discussing interruption-of-computer-services statutes).

those who prey upon the elderly's insecurities and lack of technical understanding for their own monetary gain.[185] Their intent, after all, is malicious and the end result sought, at least in the case of defrauding the elderly, is personal gain. However, as previously noted, often the threshold amount of monetary damage under these statutes is surprisingly low, thus allowing the statute to treat almost any offense as a serious felony.[186] For example, many computer fraud statutes allow the prosecution of warez trafficking and the illegal placing of long-distance calls through a computer. This is because trafficking just one piece of software (e.g., Microsoft Office or Windows XP) or placing one international long-distance call may result in damages that have an estimated valued of over two hundred dollars, or whatever threshold amount the statute sets.[187] Therefore such activity would result in a criminal prosecution of the same magnitude as a criminal who has thrived off the technological ignorance of the elderly. On another note, in the circles of the computer underground where technological prowess is the quantifiable merit that reputations are made of, hackers often prove their worth by staging pranks.[188] It is not uncommon for hackers or phone phreaks to route each other's calls through an expensive third-party telephone carrier or to entirely re-route someone's incoming calls to, for example, a payphone in South Africa. Most certainly, such pranks should be against the law, and the law ought to deter such pranks, but it hardly seems just or fair to prosecute pranksters in the same degree as a criminal whose malicious intent was to harm the elderly or render a business's sole means of income useless.

The primary difference is intent, and the law should consider the varying types of intent when meting out punishments. The intent of a teenage hacker who takes advantage of a telephone system insecurity to call a BBS in Moscow is completely different than the intent of the confidence artist who dupes an elderly couple into allowing a criminal to access their online checking account. If the law cannot distinguish between varying types of intent, but instead relies upon very low threshold amounts of damages to determine an appropriate punishment, the result is anything but appropriate. This only serves to create drastic inequities in sentences between those charged with a computer-related criminal offense and those

185. *See* discussion *supra* Part II.A (discussing current computer fraud statutes).

186. *See supra* text accompanying notes 95–96.

187. *See, e.g.*, VA. CODE ANN. § 18.2-152.3 (Michie 1996) (stating that "[i]f the value of property or services obtained is $200 or more, the crime of computer fraud shall be punishable as a Class 5 felony").

188. *See* Social Engineering Panel, H2K2, HACKERS ON PLANET EARTH 2002 (July 16, 2002) (describing before a hacker convention various pranks and exploits utilizing the telephone system), *available at* http://www.h2k2.net/panels.html#soceng.

charged with non-computer-related offenses. Legislators, then, would well serve the equitable administration of the laws by amending computer fraud statutes to take into account the specific intent of the person committing the offense and any national or state security interests at stake.

Unlawful-use-of-a-computer and computer trespass statutes have similar consequences. As previously noted, the statutory elements of unlawful use a computer and computer trespass will usually overlap such that one charge necessarily implies the other.[189] While it is desirable that statutes are directed explicitly and exclusively towards the proscription of the unlawful use of a computer and computer trespass, each statute should have distinct elements; it should not be the case that one charge necessarily implies the other. There is something inherently unfair about bootstrapping two supposedly distinct charges that are factually and technologically indistinct, and consequently increasing the severity of a defendant's punishment.

Intent is another major issue with unauthorized-use-of-a-computer and computer trespass statutes. Most statutes determine an appropriate punishment by assessing the amount of damages without even considering an offender's intent.[190] New Mexico's unauthorized use of a computer statute is a step in the right direction in that it proscribes obtaining authorization and then using the authorization for an unintended purpose.[191] However, the broad language of the statute, while narrowing the types of unauthorized uses proscribed, also does not distinguish on the basis of intent.[192] As with computer fraud, the intents of an unauthorized user may vary considerably.[193] A hacker who intrudes into a computer system to learn or explore has a much less ignoble motive than the professional operative who intrudes into a computer to obtain trade secrets or a similarly motivated advantage.

Similar to computer fraud statutes, damages in computer trespass actions are a point of contention among the perpetrators and the victims. Meting out punishment according to damage is certainly a fair method of doing so; however, assessing damages is an issue in itself. Computer trespass necessarily involves access to that which is forbidden.[194] Access in itself does not cause any real damages, or at least no more than an unannounced visitor to a home. However, access to confidential material,

189. *See supra* text accompanying notes 109–21.
190. *See supra* text accompanying notes 95.
191. N.M. STAT. ANN. § 30-45-5 (Michie 2004).
192. *See id*. (omitting any discussion of intent).
193. *See supra* text accompanying notes 128–34.
194. *See supra* text accompanying note 108.

such as computer source code, may indeed result in substantial damages.[195] Fundamental fairness requires that the law strictly monitor the methods a victim uses to assess damages. It is very easy for victims of simple computer intrusions to inflate monetary damage assessments.[196] Because so much is contingent upon damage assessments, and because the victim is in the best position to honestly determine the monetary worth of an intrusion, when damages are contested, the law should place the burden on the victim to demonstrate that it has performed a damage assessment fairly and accurately.

Consider, for instance, Kevin Mitnick's case.[197] Many refer to Kevin Mitnick as the world's most notorious computer hacker.[198] Federal agents arrested Mitnick in 1995 and charged him under various federal and state statutes with multiple offenses, one of which was unlawfully accessing Sun Microsystems' computers and viewing the source code to their yet-to-be-released Solaris operating system.[199] Sun claimed that by Mitnick viewing the source code of Solaris he, in effect, stole it, and Sun valued their loss at $80 million.[200] This caused many to doubt the veracity of Sun's claim.[201] Amazingly, Sun subsequently began giving away the same Solaris source code to educational institutions and then sold the source code to qualified developers for as little as one hundred dollars.[202] Even though many suspected that Sun inflated its $80 million damage assessment, a federal district court denied Mitnick a bail hearing,[203] and Mitnick subsequently appealed his bail application to the Supreme Court.[204] Mitnick addressed the application to Justice Stevens, who thought it important enough to refer to the Court, but nonetheless the Court denied Mitnick's application.[205] Without bail, Mitnick awaited trial for five years in a maximum security

---

195. *See* Cadence Design Sys., Inc. v. Avant! Corp., 253 F.3d 1147, 1148 (9th Cir. 2001) (treating theft of computer source code as theft of trade secrets).

196. *See* Lindsey Arent, *Did Sun Inflate Mitnick Damages*, WIRED, May 22, 1999, *available at* http://www.wired.com/news/politics/0,1283,19820,00.html (discussing the inflated damages involved in Kevin Mitnick's prosecution).

197. United States v. Mitnick, No. 97-50365, 1998 U.S. App. LEXIS 10836 (9th Cir. May 14, 1998).

198. *See* JEFF GOODELL, THE CYBERTHIEF AND THE SAMURAI, THE TRUE STORY OF KEVIN MITNICK AND THE MAN WHO HUNTED HIM DOWN, xviii (1996) (describing Kevin Mitnick as a "dangerous virus in the system," and an "evil genius").

199. Arent, *supra* note 196.

200. *Id.*

201. *Id.*

202. *Id.*

203. *See* Michael Specter, *An Ex-Con Logs On*, THE NEW YORKER, Feb. 3, 2003, at 32 (noting that Mitnick's notoriety was probably responsible for his lack of a bail hearing).

204. Mitnick v. United States, 525 U.S. 946 (1998).

205. *Id.*

federal detention center in Los Angeles, and eventually agreed to a plea agreement.[206] Mitnick's plight demonstrates the inequity of the cybercrime system—with the ability to inflate the value of damages, and without any mechanism to verify the accuracy of those alleged damages, excessive and inaccurate damage assessments can result in the prosecution of the most trivial computer trespasses as if they were the most grievous of crimes.

Computer trespass for the sake of trespassing is certainly wrong, but in the absence of malicious intent or reckless acts, there is no serious harm. Such conduct should be free from draconian legal repercussions. States should take note of Nevada's sensible approach in meting out punishments proportional to the public risk involved in a computer trespass.[207] In this sense, the state expressly protects its own welfare and that of its citizens. Computer intrusion into the network of Sun Microsystems, without more, would not be tantamount to a computer intrusion into a power utility's computer network or a military network.[208] While the law must punish intrusions of the former kind, fairness dictates that the law should punish more severely those whose crimes threaten to affect the national security than those who trespass merely for the sake of trespassing. The difference between these two offenders is that one commits a crime in furtherance of knowledge and because of curiosity, and the other commits a crime in furtherance of terror and because of animosity. Without a distinction between these types of offenders, cybercrime statutes cannot mete out equitable treatment under the law.

Interruption-of-computer-services statutes undoubtedly serve the most vital interests. DoS and DDoS attacks can be devastating and seriously undermine the welfare of a state if directed towards vital targets. Furthermore, the ease with which criminals can carry out DoS and DDoS attacks, and the various forms such attacks may take, are pressing concerns of a state. Because of this threat, statutes specifically proscribing and criminalizing the interruption of computer services by way of DoS, DDoS, or malicious computer viruses and worms, are very well-intentioned statutes. Nonetheless, the severity of the punishment should be proportional to both the intent of the attacker and the harm inflicted.

---

206. *See* Gail Diane Cox, *Famed Hacker Fights for His Right to Seek Fortune*, LEGAL TIMES, May 15, 2000, at 15 (describing the facts of Mitnick's case and his subsequent attempts at securing employment after his release from prison).

207. Unlawful Acts Regarding Computers, NEV. REV. STAT. ANN. § 205.4765 (2001 & Supp. 2003).

208. *See* § 205.4765.6(c) (providing harsher punishments only for the unlawful use of computers intended to disrupt a public service or government operation).

For instance, does it make sense to prosecute those responsible for the ElectroHippies' DoS attack on the World Economic Forum's website in the same manner as a criminal who would launch a global DDoS attack directed towards computer networks of the U.S. government? Any DoS attack is objectively wrong and illegal even if it serves primarily as some form of political statement of dissent or disagreement. Civilly disobedient acts require punishment to fully draw attention to the protested policies and complete the disobedient act.[209] But there is a tremendous difference of intent between "hacktivism" stunts intended to convey a message by temporarily disabling a commercial website and directing a DDoS attack towards targets of national interest. The former benefits from the message, and the latter benefits from the harm. Similarly, the former criminal act has a very narrow and focused scope of harm, while the latter's harm is intentionally broad and malicious. The law should punish less severely those who employ DDoS attacks without intending irreparable harm. It is inequitable to punish them in the same manner as those who use DDoS attacks as weapons of war or terror. Currently, however, the law does not distinguish between the two crimes and their intents.

Interruption-of-computer-services statutes also intend to curtail reckless actions, and rightly so. Anyone who engages in DoS or DDoS attacks, or who releases a Trojan or self-replicating worm, invariably places many at risk by their actions. However, the level of moral culpability will vary considerably. Consider the following scenario: a disgruntled computer hacker and cellular service customer devises a large scale DDoS attack against his cellular carrier for what he believes were fraudulent billing practices. The hacker employs the use of 10,000 zombie computer systems located all over the world and targets the cellular provider's network operations center in New York City because it handles both voice and data operations. The DDoS attack is incredibly successful, and as a consequence, customers cannot place voice calls over the cellular carrier's network and data operations in lower Manhattan are completely halted for twelve hours. Hundreds of thousands of customers are without phone and data service causing the aggregate loss in business to total $10 million.

Consider the same situation in which the hacker, for the same underlying reasons set forth above, targets the same cellular carrier's network in New York City, but entirely because he believes it is only the voice center of operations. The same exact consequences ensue.

---

209. *See* RONALD DWORKIN, *Civil Disobedience*, *in* TAKING RIGHTS SERIOUSLY 206–23 (1978) (discussing the philosophy of civil disobedience generally and the requirement of punishment).

Both scenarios have the same result, but the former is more morally culpable and reprehensible than the latter. In the former scenario, the consequence was both foreseeable and intentional; on the other hand, the latter situation's consequences were foreseeable but unintentional, and therefore less morally reprehensible. The Catholic Church calls this doctrine the principle of double effect.[210] This principle is particularly relevant to the effects of DDoS attacks and the release of worms because it underscores how intent determines varying levels of culpability. Further, the principle of double effect also demonstrates why the law ought not to punish harmful conduct that is foreseeable but unintentional as severely as conduct that is intentional and foreseeable. In short, to equitably administer punishment, there must be an assessment of the nature and extent of harm resulting from DoS, DDoS, Trojans, and worms, together with the intent of the individual who devised the scheme. Only then can the law avoid excessive punishments wholly out of proportion with the extent of the harm and an offender's intentions.

Currently, the law makes no such distinctions. Even for the most trivial reckless offenses involving slight harm, the law requires harsh criminal punishment.[211] Undoubtedly, this may have a strong deterrent effect, but so too would the imposition of harsh monetary sanctions.[212] The law would punish well a computer hacker whose actions do not cause substantial damage and whose actions are not a national security threat by requiring payment of restitution, probation, and a hefty fine. Doing otherwise imprisons youth for what often is the result of youthful indiscretion and poor judgment. Consider the absurdity of a real-space analogue: a law that punishes a first-time, unintentional, yet foreseeable, trespass as a felony carrying a punishment of over one year imprisonment. None would argue that this trivial act warrants such a harsh punishment.

The law is quick to punish trivial transgressors, but apparently refuses to punish those who create the dangerous situations that allow potentially hazardous transgressions to occur in the first place. What warrants further consideration is why it is so easy to commit crimes that may result in incredible harm to our nation's information infrastructure. Any computer

---

210. *See generally* Warren S. Quinn, *Actions, Intentions, and Consequences: The Doctrine of Double Effect*, *in* 18 PHILOSOPHY AND PUBLIC AFFAIRS 334–51 (1989), *reprinted in* THE DOCTRINE OF DOUBLE EFFECT 23–40 (P.A. Woodward ed., 2001) (compiling various philosophers' interpretations and analyses of the controversial moral principle of double effect).

211. *See supra* text accompanying note 94.

212. *See* Vern Krishna, *Tax Views: Insider Trading and Tipping*, THE LAWYERS WEEKLY, Feb. 21, 2003, at 39 (discussing the harsh monetary sanctions for misappropriating confidential information in the context of insider trading and arguing that harsher penalties directly benefiting the adversely affected investors would be an even stronger deterrent).

hacker worth his salt may perform a DoS or even a DDoS attack.[213] Any programmer worth his salt can create a self-replicating worm, capable of bringing networks to a near halt.[214] The reason for this is deceptively simple: there is never a shortage of Windows security holes.[215]

Microsoft's Windows operating system controls the vast majority of the operating system market: 97.46%.[216] Therefore, when a security hole that allows remote access or facilitates DoS attacks becomes public knowledge, the vast majority of the world's computer systems and networks are at risk. Almost every worm and every Trojan has preyed entirely upon known, and often glaring, security holes in the Windows operating system.[217] Eventually Microsoft's programmers address and correct these vulnerabilities: after Microsoft officially acknowledges that a security hole exists, assembles a task force, devises a patch, distributes the patch (sometimes for a fee), and system administrators the entire world over install the patch and update their systems.[218] In reality, system administrators are busy people, often in charge of hundreds or thousands of computers, and patching security holes invariably takes the backseat to a host of more pressing issues.[219] The result is that millions of computers worldwide remain unpatched, unprotected, and vulnerable to attack.[220]

The cause of such insecurity is the poor programming of the Windows operating system. Microsoft, in its usual hurry to release the next version of Windows, inevitably releases an incomplete and insecure product.[221] Of course, if a company sought to release perfect software, it would never release anything. Software is by its very nature a finicky product, and will always have its flaws.[222] But, cautious quality assurance mechanisms in

---

213. *See* Bland_inquistor *supra* note 135, at 41 (discussing available mechanisms to accomplish DoS and DDoS attacks).

214. *Id.*

215. Livingston, *supra* note 167, at 39.

216. *Microsoft's Windows OS Global Marketshare Is More Than 97% According to OneStat.com*, *at* http://www.onestat.com/html/aboutus_pressbox10.html (last visited July 29, 2005).

217. *See* Livingston, *supra* note 167, at 39 (discussing the many security vulnerabilities in the Windows-based webserver, IIS, that allow the creation of Internet worms). There is one notable exception: Robert Morris' Internet worm devised in 1988 utilized a known security hole in the UNIX sendmail program. *See* Jonathan Littman, *The Shockwave Rider: Background on Robert T. Morris Jr., Author of the Internet 'Worm'*, 3 PC-COMPUTING 142 (1990) (discussing in great depth Morris' background and proliferation of the first Internet worm).

218. *See* Scott Berinato, *FrankenPatch*, CIO MAGAZINE, Nov. 1, 2003 (discussing the terribly complex system of patching security holes and the need to develop better patching techniques), *available at* http://www.cio.com/archive/110103/security.html.

219. *Id.*

220. *Id.*

221. *See* Livingston, *supra* note 167, at 39.

222. *See* Berinato, *supra* note 218 (noting that the immense number of software flaws creates a

place at the design level, together with setting a higher priority for information security, could have avoided many of Windows' eminently foreseeable security holes.[223]

Because of its market share and copious vulnerabilities, Microsoft's Windows operating system is the nation's largest threat to its information infrastructure.[224] However, Microsoft has yet to face any liability for its faulty products. Recent lawsuits seek to change this: a California woman has sued Microsoft alleging that flaws in its operating system caused her to be the victim of identity theft.[225] The plaintiff and her lawyers seek to turn the lawsuit into a class action and represent the many who have suffered at the hands of Microsoft's alleged data security negligence.[226] The courts have not yet addressed the issue of software liability for security vulnerabilities, and this case may open or completely shut the floodgates for many potential plaintiffs. The arguments in favor and in opposition for software liability merit consideration.

The government should not so easily countenance the creation of software placing individual and national interests at risk. Legislators ought to contemplate the potential liability software vendors have for security flaws that are foreseeable and could cause much harm. Arguably the chain of causation of cybercrimes extends back to the vendors of software, and therefore necessitates some form of responsibility.[227] Liability should exist for those who make value judgments that place information security on the low rung of the ladder and thereby create the means by which criminals may accomplish cyberattacks or cybercrimes.

In fairness, it is not right for Microsoft to bear the burden entirely—computer users are also partly to blame. Users have the responsibility to be aware of security concerns and install security patches that are available.[228]

---

patching volume problem).

223. *Id.*

224. *See supra* note 216 and accompanying text.

225. Richard Hunter, *Lawsuit Challenges Wall Protecting Software Vendors From Liability* (Oct. 9, 2003), *available at* http://www.gartner.com/resources/117800/117829/117829.pdf. Many of the specifics regarding this lawsuit are as of yet unavailable on the Los Angeles Superior Court's docket; therefore, the information presented derives from the current sources available. What is currently known is that the plaintiff, Marcy Levin Hamilton, and her attorney, Dana Taschner, are suing Microsoft alleging: 1) that Microsoft is a monopoly; 2) that consumers have no recourse when criminals can exploit known security vulnerabilities; 3) that Microsoft does not have an adequate system to notify its customers of security vulnerabilities. *American Morning*, Interview by Bill Hemmer with Marcy Levin Hamilton, Plaintiff, and Dana Taschner, Attorney, in New York, N.Y. (CNN television broadcast, Nov. 6, 2003), *transcript available at* http://www.cnn.com/TRANSCRIPTS/0311/06/ltm.12.html.

226. *American Morning*, *supra* note 225.

227. *Id.*

228. Jaikumar Vijayan, *Improved Security Through IT Diversity*, COMPUTERWORLD, Nov. 24, 2003, at 28.

What courts must decide is how much contributory negligence each party is responsible for, and award damages accordingly.[229] Some argue that imposing liability for security vulnerabilities on software companies is bad public policy because the costs of litigation and damages would be passed onto the customer.[230] Further still, if software companies are potentially liable for their programming flaws, they may be hesitant to release new products.[231] In this sense, software liability may significantly hinder innovation and dull the competitive edge of the U. S. software industry.[232]

Once a software giant like Microsoft is liable for its software vulnerabilities, it is certain that decision-makers will start taking the security and privacy of its customers more seriously.[233] Without the economic incentive to do so, software companies will continue to consider information security as a low priority.[234] While there is some merit to the argument that software liability may hinder the innovation of U.S. software companies, it would simultaneously promote innovation within the open-source community.[235] Holding software companies liable for their security vulnerabilities may cause Microsoft much headache, but open source products, such as Linux, would benefit from their open development model and the way in which it encourages widespread peer-review.[236] The peer-review methodology of open source software creates products that are more secure and stable than traditional closed source products like Microsoft's Windows operating system.[237] The theory is that when anyone can see how the program operates, users the world over can fix potential security vulnerabilities before they become major problems.[238] Software whose patent holders keep its source code a closely guarded secret can never benefit from this peer-review system. When there are more secure and

---

229. *Id.*

230. *See* Todd Bishop, *Should Microsoft Be Liable For Bugs?*, THE SEATTLE POST-INTELLIGENCER, Sept. 12, 2003, at A1 (weighing the benefits and costs of holding software companies liable for their programming flaws).

231. *Id.*

232. *Id.*

233. Vijayan, *supra* note 228, at 28.

234. *Id.*

235. Programmers acting collaboratively to create software and adhering to strict licensing agreements that require the computer source code of a program to be freely available to the public create what is commonly known as open source software. The most notable example of open source software is the Linux operating system; the media has recently focused much attention on Linux as a rival to Microsoft Windows. *See* Webopedia, Small Business Computing Online Dictionary of IT Terms, *at* http://sbc.webopedia.com/TERM/L/Linux.html (last visited July 29, 2005).

236. Andrew Leonard, *Life or Death Software*, Aug. 5, 1999, *at* http://archive.salon.com/tech/feature/1999/08/05/anesthesia/.

237. *Id.*

238. *Id.*

reliable software alternatives available, it does not make sense to reward companies with immunity for their flaws and to perpetuate a system that creates insecure software.

Legislators should not be concerned with sustaining the profits of software giants when the interests at stake are national security and the nation's information infrastructure. In addition to punishing those who engage in cybercrimes by criminally exploiting known security holes, it is high time to create new statutes that punish, with substantial monetary penalties, those software companies whose errors and omissions place the nation and its citizens at risk.

CONCLUSION

As technology's ubiquity continues to change our lives and our society, it too will change the nature, and possibly the definitions, of crimes and criminals. That criminals may one day carry out a devastating cyberattack directed towards this nation's information infrastructure is no doubt a frightening prospect, but the principles of fairness and equity must always be the driving force behind the law. Similar to Operation Sundevil in its most nascent stage of a rapidly evolving area of criminal law, the interests involved in our nation's modern approaches to ever-changing cybercrimes will hopefully progress in the right direction.

Only by removing the draconian penalties associated with trivial acts, incorporating accurate and measurable mechanisms to assess harm and monetary damages, and allowing for the proper consideration of the intent behind a particular cybercrime, will our nation's response reflect our richer understanding of temperance, equity, and justice. Only by giving software companies like Microsoft an incentive to create software without glaring security holes will the nation's and the world's problems of information security and cybercrime begin to subside. Without such modifications in our approach, our nation's laudable, albeit knee-jerk, reaction to a new genre of difficult technological and legal problems will continue to irreparably and unnecessarily harm the young and precocious because of their innate curiosity, questionable judgments and youthful mistakes.

Alexander Urbelis