FOCUS - 1 of 1 DOCUMENT

The Transnational Lawyer

Spring, 2001

14 Transnat'l Law. 135

LENGTH: 17415 words

COMMENT: **Prosecuting Computer Virus Authors:** The Need for an Adequate and Immediate International Solution

NAME: Kelly Cesare*

BIO: * J.D., University of the Pacific, McGeorge School of Law, to be conferred May, 2002; B.A., Communication, University of Southern California, 1999. I would like to thank Andrew Nelson for his countless hours of patience and assistance; his guidance and sense of humor made the entire writing process enjoyable for me. I would also like to thank my parents and friends for their constant love, faith, encouragement and support, especially my roommate, Gina Nargie, for putting up with me and my inability to keep our apartment tidy during Fast Trak.

SUMMARY:
... However, a new villain - the virus author - has surfaced, bringing a new crime into the international forum: the spread of the computer virus. ... Free from the fear of prosecution, the virus author feels no need to stop wreaking global havoc. ... Part II focuses on the crime of the spread of a computer virus and the type of damage that a virus author is capable of inflicting across the world from a single isolated terminal. ... Finally, the section concludes with an overview of the role a virus author plays in instigating that crime. ... Computer crime legislation as a whole covers a wide variety of offenses. ... For the United States, the Melissa virus concluded with "the first successful prosecution of a virus author in over a decade and only the second successful prosecution in [American] history" under the nation's specialized computer crime statutes. ... Countries with Lesser Computer Crime Laws ... " Certain aspects of computer crime legislation are particularly incompatible with extradition. ... This roadblock kept the United States from extraditing the ILOVEYOU virus author from the Philippines. ... Some government efforts do not require help from the private sector to combat computer crime. ...

TEXT:
[*136]

I. Introduction

Imagine the following scenario: a disgruntled employee [n1] decides to take it upon herself to seek revenge on her employer corporation. She secretly creates a strand of malicious computer code [n2] that will damage any computer it infects. [n3] From her home computer, the employee uses her dial-up modem [n4] to access [n5] the corporation's computer system and releases the code into it, destroying data on every company computer that becomes infected and completing her mission of revenge. However, the nightmare does not end here. Unbeknownst to anyone, including the culprit, co-workers that are working from infected terminals are perpetuating the malicious [*137] code with every e-mail [n6] they send [n7] through the Internet. [n8] The code reaches countless computer terminals, irrespective of jurisdictional and sovereign boundaries. The code causes millions of dollars in damage throughout the world before it can be quashed. But the greater injustice resulting from this scenario has yet to be realized: the country in which the disgruntled employee resides has no law under which to prosecute her act, and her extradition to a country which does is unfeasible. She

emerges unpunished by the law. What may sound like an imaginary plot for a dramatic movie is unfortunately an all too real scenario, reflective of how a computer virus [n9] proliferates into a worldwide problem.

International borders have long been a stumbling block in the successful prosecution of crimes. There are a number of common scenarios that illustrate this point: an individual may commit a crime in one country, then flee to another, in an attempt to escape the law; she may commit an act in a country that does not consider the action criminal; [n10] or she may act in one country, which produces effects in another. [n11] Any of these three generalizations lead to prosecutorial problems for the countries involved. Questions of jurisdiction are inevitably invoked.

In response to jurisdictional problems, the world engineered a solution: extradition. [n12] Extradition works because most nations prosecute the same types of crimes, although the severity of punishment varies from country to country. [n13] Deterring crime is an underlying policy goal for the enactment of all laws. [n14] Through [*138] extradition, an international criminal can run but cannot hide. The deterrent effect of criminal laws are thereby strengthened.

However, a new villain - the virus author [n15] - has surfaced, bringing a new crime into the international forum: the spread of the computer virus. [n16] However, she escapes prosecution [n17] largely because many countries simply have no cyber [n18] crime laws. Therefore, extradition is not a viable prosecutorial alternative. Free from the fear of prosecution, the virus author feels no need to stop wreaking global havoc.

This Comment addresses the hardships experienced by nations around the world in attempting to prosecute virus authors. Ultimately, this Comment argues that among the numerous proposals attempting to address the problem, the Council of Europe's draft Cyber-Crime Treaty [n19] is the best solution offered thus far. Part II focuses on the crime of the spread of a computer virus and the type of damage that a virus author is capable of inflicting across the world from a single isolated terminal. This section goes on to discuss the current state of cyber crime laws, or lack thereof, in the United States and other nations, and their level of success in prosecuting virus authors. Part III discusses the difficulty in prosecuting cyber criminals, illustrating this with a few examples from recent history. Part IV evaluates some solutions proposed by various parties and gives a detailed description of the relevant sections of the Council of Europe's proposed solution: a draft Cyber-Crime Treaty. Finally, Part V concludes that, despite its minor flaws, the Council of Europe's draft Cyber-Crime Treaty is the most efficient and effective way to effect immediate change in light of the other proposed solutions.

II. The Crime of the Computer Virus

Because the spread of a computer virus is still a relatively new crime, understanding the mechanics of a malicious code is a precursor to demonstrating how the computer virus can be used as an instrument of crime. Upon concluding that some type of conduct relating to computer use may be criminal in nature, the next step is to identify how modern criminal law systems might be better equipped to deal with the problem. Examples of recent virus outbreaks help illustrate why the spread of computer viruses constitutes criminal conduct, which necessitates strong prosecutorial strategies.

[*139]

A. The New Crime: The Computer Virus

This section begins by outlining the basics of a computer virus. [n20] It then discusses how a computer virus is used to facilitate a crime. [n21] Finally, the section concludes with an overview of the role a virus author plays in instigating that crime. [n22]

1. What is a Computer Virus?

A virus is one species of a malicious computer code [n23] "written with the sole intent to cause damage to a machine or to

invade the machine to steal information." [n24] "A virus is a program that infects a computer by inserting a copy of itself into the computer and harms the computer in some manner, generally without the computer user's awareness." [n25] Viruses can be harmful or benign. [n26] The typical mode of distributing a virus is via e-mail or an infected disk, [n27] but a virus cannot infect a computer until the program is executed. [n28] Usually the unknowing recipient is duped into opening an attached file in an e-mail or a file contained on a disk, thinking it is [*140] harmless and/or it came from a friendly source. [n29] Hiding a "macro" [n30] routine in a common Microsoft Office product file, such as Word or Excel where the macro tells the computer to perform harmful actions, is another way a virus can be executed. [n31] Only files that are "executable" (.exe) [n32] are capable of transmitting a virus, whereas, data files, such as image (.jpg and .gif), music (.wav and .mp3) or text (.txt) files are not capable of transmitting a virus because they do not contain macro functionality, [n33] or they cannot command the computer to perform any functions. [n34] Once a virus is activated, the damage or interference it causes is not always immediate or apparent. [n35] An author can design a virus to trigger in countless ways, [n36] and individuals are constantly inventing new triggering mechanisms. There are several places a virus can hide within a host computer, [n37] and once the virus infiltrates a computer, it can replicate and spread itself without further assistance from the user. [n38] Once triggered, the damage that a virus causes is referred to as the "payload." [n39] When the virus infects the hard drive, [n40] its payload launches. The [*141] damaging interference that results can range from "annoyingly humorous ... to total devastation" of the hard drive. [n41]

2. The Role of the Computer Virus in Criminal Law

Computer crime legislation as a whole covers a wide variety of offenses. [n42] Since computer crime legislation is still relatively new, [n43] it is necessary to understand precisely how the proliferation of a virus constitutes computer crime. As computer viruses began to evolve into serious security and financial threats, lawmakers began criminalizing their distribution. In the United States, merely writing a piece of malicious code is not a crime without the necessary intent to access an unauthorized computer. [n44] To constitute a punishable offense, the virus must be knowingly transmitted to another computer, via e-mail, infected disk, or otherwise.

When computer crimes were first recognized, they were simply encompassed by traditional crimes, the only difference being that the crime was being committed with the aid of a computer. [n45] As technology advanced, however, it became apparent that new computer crimes, such as the intentional spread of viruses, were unique to computers and thus needed particularized legislation. [n46] There is an ongoing debate in today's world as to whether such legislation is in fact necessary because a great number of crimes committed with the use of a computer can be prosecuted under traditional statutes already in existence.

[*142] Legal scholars and law enforcement experts differ in opinion as to where cyber crimes fit within modern criminal law. [n47] Some experts believe that computer crimes, including the mischievous use of viruses, are simply traditional crimes committed with advanced technology, and current criminal laws suffice to punish computer crimes. [n48] Other experts believe that cyber crimes are a new category of crime requiring a comprehensive, separate legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not address. [n49]

In the United States, there are many statutes from which a federal prosecutor can choose when prosecuting a computer criminal. [n50] Sometimes, a prosecutor uses a traditional statute to prosecute a computer-related offense. For example, the federal Copyright Infringement Act, *17 U.S.C. 506* can be used to prosecute a copyright violation, despite the fact that a person used a computer to facilitate the crime. Other times, a prosecutor may utilize a new computer crime statute, tailor-made for crimes that cannot be committed absent the aid of a computer. An example of such a statute is the National Information Infrastructure Protection Act. [n51] The prosecutor's choice depends on the circumstances surrounding the crime and which statute is most likely to lead to a successful prosecution. [n52] However, one country with a statute tailor-made to combat cyber crime is not always the answer. [n53]

[*143]

3. Illustrative Examples of Recent Virus Outbreaks

As technology advances, individuals consistently find ways to exploit it for deviant purposes. [n54] The vast majority of intrusive hacking is done for research purposes, such as investigating breaches in security. [n55] There are those, however, that use their software and computer talents in a mischievous manner, launching computer viruses for purposes that are criminal in nature. [n56] Some reports attribute major financial and security threats to the ever-increasing volume of new viruses released on the Internet each year. [n57] These virus releases can originate from any location equipped with a telephone line, and the effects can vary widely. The act of releasing a computer virus contains the basic elements of what makes certain conduct criminal, namely community condemnation and moral delinquency. [n58]

a. Melissa

The Melissa virus first surfaced in March 1999, rapidly infecting computers across the world and causing eighty billion dollars in damages. [n59] Melissa was the fastest-spreading virus the United States had ever seen, hitting over one hundred thousand U.S. computers in just a few days. [n60] The virus spread via e-mail, invading users' address books and sending up to fifty e-mail messages to addresses stored on the infected computer. [n61] The virus enticed the user into opening an attachment with the message subject header "Important Message from (the name of someone on the [*144] list)." [n62] Melissa spread rapidly, and within forty-eight hours major companies such as Microsoft and Intel were forced to shut down their servers. [n63]

b. Chernobyl

April 26, 1999 marked the thirteenth anniversary of Russia's Chernobyl nuclear power plant meltdown, and the day Chen Ing-hau chose to trigger a release of his virus of the same name causing "a meltdown of a different kind." [n64] The virus "Chernobyl" or "CIH" [n65] was a particularly frightening virus because its infection actually damages a computer, rendering it physically inoperable. [n66] Infecting computers running Windows 95 and 98, Chernobyl "deleted data on a computer's hard drive and attempted to overwrite and destroy a PC's flash BIOS, which [are] needed to boot the computer." [n67]

Although Chernobyl "paralyzed" sixty million computers across the globe, [n68] it scarcely affected the United States. [n69] Since the recent Melissa virus disaster, [n70] U.S. companies improved their virus protection strategies that successfully shielded them from the Chernobyl virus. [n71] However, as the rest of the world was uninformed about the Melissa virus and therefore unaware of the need to improve its technology, [*145] Chernobyl hit the rest of the world hard, with Asia suffering the most serious damages. [n72]

c. ILOVEYOU

On May 4, 2000, the Internet experienced a monumental disaster when the ILOVEYOU virus surfaced, infecting millions of computer files around the world. [n73] The virus, which quickly earned the nickname the "Love Bug" due to the "I Love You" phrase displayed in the subject-matter heading of each contaminated e-mail, [n74] activates when the e-mail attachment is downloaded, thereby destroying image and sound files stored in the computer. [n75] After infecting the terminal, it spreads by automatically sending the e-mail to everyone in the infected computer's address book and thus causing widespread infection. [n76] The "Love Bug" reportedly attacked only Microsoft Windows operating systems, the dominant operating systems among personal computers and where most e-mails are downloaded. [n77] Conservative estimates show the loss directly attributed to the ILOVEYOU virus at around ten billion dollars. [n78]

B. Current Laws and Levels of Success

"All nations continue to struggle with defining computer crime and developing computer crime legislation that is applicable to both domestic and international audiences." [n79] Unfortunately, countries are not advancing at equal speeds, and virus authors are taking advantage of those countries making slower progress. [n80] Understanding the vast

gap in the legislative advances of some nations when compared to others leads to the conclusion that more must be done on an international level in order to effectuate successful cyber crime prosecutions.

[*146]

1. United States Law

There are at least forty different statutes in the United States under which computer criminals can be charged. [n81] The United States realized that some offenses such as viruses are unique to computers and require prosecution under specialized statutes tailored to computer related activities. [n82] Therefore, the United States has treated cyber crime as a distinct federal offense since 1984. [n83] Throughout the 1980s [n84] and 1990s, [n85] Congress amended cyber crime statutes to reflect the growth in the number and breadth of diversity of cyber crimes. [n86] In 1996, Congress passed the National Information Infrastructure Protection Act (NIIPA) *18 U.S.C. 1030* which contains the most recent changes and modifications to the Counterfeit Access Device and Computer Fraud and Abuse Law. [n87] The statute, which previously only covered crimes involving computers in more than one state, now covers any computer with Internet access, even if all the computers involved in the crime are located within one state. [n88]

[*147] For virus authors, the relevant portion of NIIPA is section 1030(a)(5), which criminalizes knowingly causing the transmission of a program, code, or command with the intent to cause damage. [n89] Sections 1030(a)(5)(B) and (C) criminalize the intentional accessing of a computer in excess of one's authority, [n90] and causing damage as a result of that conduct, regardless of intent. Therefore, "unauthorized users, such as hackers who cause the transmission of malevolent software, including viruses, are responsible even if the transmission was not intentional, but only reckless or negligent." [n91] The newest version of the legislation removes some of the possible defenses a virus author could raise under earlier versions regarding jurisdiction, intent, and the amount of damages she was required to inflict. [n92]

For the United States, the Melissa virus concluded with "the first successful prosecution of a virus author in over a decade and only the second successful prosecution in [American] history" [n93] under the nation's specialized computer crime statutes. As a result of an extensive search, the virus author, David Smith, was apprehended within a few days of Melissa's appearance. [n94] He pled guilty to state [n95] [*148] and federal charges of causing computer damage, [n96] which included an admission that he was responsible for the eighty million dollars in damages to over a million affected computers. [n97] Smith is still awaiting sentencing for the crime, [n98] despite being found guilty in late 1999. [n99] He could receive several years in prison and a fine of hundreds of thousands of dollars. [n100]

2. Countries with Lesser Computer Crime Laws

While the United States and other technology-dependent countries are drafting sophisticated computer legislation, the majority of countries are not. Outbreaks of damaging and fast-spreading viruses, such as Chernobyl and ILOVEYOU, are illustrative of two countries that have inadequate criminal protection against the spread of computer viruses.

When Chernobyl first surfaced in 1999, military authorities briefly questioned its author, Chen Ing-hau, yet he evaded punishment because Taiwanese companies failed to file complaints. [n101] However, when the virus surfaced again in April of 2000, a Taiwanese resident filed criminal charges after the virus infected his computer, [n102] and Ing-hau was thereafter arrested by Taiwanese authorities. [n103] Since Taiwan does not have a cyber crime law, the Bureau of Criminal Investigation charged him with offenses of destruction and damage. [n104] If convicted, Ing-hau faces a maximum sentence of three years. [n105]

While Ing-hau's arrest is a positive step toward dealing with computer crime, it falls short of the success that legislation specifically designed to combat computer crime can accomplish. [n106] Taiwan depended on someone stepping forward to file formal charges, [n107] fortunately giving the country a second opportunity to prosecute [*149] the virus author. If a law existed that defined Ing-hau's act of intentionally releasing a computer virus onto the Internet as criminal, the government could have prosecuted him over a year earlier, instead of being forced to wait for a civil

complaint to surface.

When the ILOVEYOU virus surfaced in May 2000, the Philippines found itself in a situation similar to Taiwan's: an apprehended culprit but no adequate criminal statute under which to charge him. The National Bureau of Investigation (NBI) charged Onel de Guzman, the suspected author of the "Love Bug," [n108] with theft, malicious intent, and violation of the Philippines Access Devices Regulation Act, [n109] which carries penalties of six to twenty years imprisonment. [n110] The Department of Justice Panel reviewed the case and was left with no alternative but to clear De Guzman of all charges because a prima facie case could not be established. [n111] One of the member-prosecutors of the three-man panel commented that the charges of theft and malicious intent were bound to fail because "the NBI failed to provide evidences of the suspect's intent to gain or inflict injury." [n112] Philippine authorities released de Guzman, and dismissed his formal charges due to a lack of evidence and a lack of a specific law criminalizing computer hacking. [n113]

The Philippines' embarrassment following the release of this cyber criminal motivated the government to quickly write and pass the Electronic Commerce Act of 2000, [n114] legislation that could have facilitated de Guzman's prosecution if it had [*150] been in place at the time he committed his act. [n115] Although the new piece of legislation came too late to adequately handle the ILOVEYOU disaster, the Philippines is now equipped to deal with such a problem should it arise again.

Although the Philippines is now prepared to combat cyber crime, other virus havens [n116] continue to exist around the world. Passing the Electronic Commerce Act of 2000, ensured that the Philippines would no longer be one of these havens, but this is not sufficient to deal with the global threat cyber crimes present. A coordinated international solution is required.

III. The Problem: Enforcement and Extradition

Today, countries worldwide are learning the hard way that their domestic laws are inadequate when attempting to prosecute virus authors located on foreign soil. [n117] "Cyberspace has no geographic or political boundaries." [n118] The ease with which viruses spread allows virus authors to perpetrate their criminal conduct in one country and simply watch their handiwork spread across national boundaries. Recent Internet virus outbreaks [n119] and the difficulties many countries faced attempting to [*151] bring the responsible authors to justice demonstrate the ineffectiveness of the current international system. It is evident that only laws which transcend physical boundaries can remedy this ongoing problem.

A. Enforcement Problems

Although countries like the United States drafted specially-tailored laws to aid in the prosecution of computer crimes, very few indictments have actually resulted. [n120] One reason for this prosecutorial lag may be that until 1996, prosecution under the Computer Fraud and Abuse Act depended on the type of computer that the virus affected. [n121] Another reason may be that those who own statutorily protected computers often do not report security problems for fear that it would spotlight the vulnerability of their computers and cause them to lose business. [n122] In addition, there is the difficulty inherent in tracking down a culprit. [n123] This may be attributable to both the ease with which one can maintain anonymity on the Internet [n124] and the lack of specially trained or experienced agents skilled to investigate complex computer [*152] crimes. [n125] Together these factors prevent countries from bringing perpetrators of computer-related crimes to justice.

Inability to quickly apprehend a perpetrator may also result in enforcement problems. When a search is underway for a cyber criminal, countries depend on the assistance of the international community. More often than not, countries are unable to respond quickly to each other, causing setbacks to a fast-paced investigation. [n126] When a country is forced to request international assistance to handle a developing situation the complex nature of the legal process or a lack of amicable relations between countries sometimes causes a loss of momentum. These types of impediments can result in suspending an entire investigation for weeks, sometimes months. [n127] Most countries agree that eliminating the

time-consuming red tape that often interferes with an investigation is necessary to ensure a more rapid response to cyber events. [n128]

Although chronologically, Melissa was one of the first major viruses to appear on the Internet, Melissa is an outstanding illustration of effective cooperation between law enforcement and the Internet community. David Smith was identified through the collaborative efforts of private companies, individual Internet users in Sweden and the United States, [n129] America Online, and federal and state law enforcement. [n130]

[*153] Before concluding that Smith's successful prosecution is a result of seamless international cooperation, the underlying circumstances require a closer look. The success and ease with which Smith was apprehended may be due to his choice of authoring Melissa in the United States and remaining in the country until apprehended. The United States, a country with a specialized cyber crime law firmly in place, [n131] was well-equipped statutorily to handle the situation once Smith was caught. If Smith had authored Melissa in a country without a cyber crime law or fled to one after releasing the virus, it is less likely he would have been prosecuted. [n132] Lack of extradition treaties also aid virus authors in escaping the not-so-long arm of the law.

B. Extradition

Extradition [n133] and laws governing computer crimes share a common characteristic: both are "hopelessly outdated and therefore, lagging behind the forces they are trying to regulate." [n134] Certain aspects of computer crime legislation are particularly incompatible with extradition. [n135] Some countries liberally interpret treaties to allow for extradition while others such as the United States require more formal arrangements. [n136]

While the United States has entered into numerous treaties with countries all over the globe, [n137] U.S. extradition arrangements share many basics traits. The traits [*154] relevant to the extradition of cyber criminals are reciprocity, [n138] a treaty, [n139] and double criminality. [n140]

Reciprocity is more a function of one nation's goodwill toward another, rather than a technical treaty provision. [n141] Reciprocity rests on the notion that if one nation honors another country's request for extradition, the requesting nation will do likewise when the situation is reversed. [n142] Reciprocity is most often a critical factor when no treaty exists between the two countries. [n143] However, countries such as the United States that require an actual treaty to be in place for any extradition, will always refuse extradition to a country with whom it has no treaty, regardless of goodwill considerations. [n144]

"Double criminality requires that the offense charged be considered criminal in both the requesting and requested jurisdictions." [n145] Originally, the double criminality provision [n146] in a treaty stood for securing fundamental rights for the individual. [n147] Now it functions as a loophole that allows computer criminals to escape prosecution. [n148] Although most nations agree that spreading computer viruses should be illegal, extradition is difficult because of disagreement over the severity of punishment and precisely what is regulated. [n149]

[*155] Historically, extradition treaties listed extraditable offenses, ensuring that only those particular crimes required a country to hand over a criminal. [n150] A major drawback of this approach is its inability to respond to substantive changes in the law. Many countries realized this and amended existing extradition treaties to utilize the "eliminative method," where actions are extraditable if under both countries' laws the action carries a specified minimum level of punishment, [n151] usually one year. [n152]

However, even the eliminative approach contains obstacles, particularly with regard to computer crimes. When such novel crimes are at issue, it becomes impossible to measure the length of a sentence under one country's law against another country's because the latter may not consider the act criminal. [n153] This roadblock kept the United States from extraditing the ILOVEYOU virus author from the Philippines. [n154] Although the majority of countries today criminalize computer crimes, [n155] the lack of legal uniformity causes serious extradition problems. [n156]

Regardless of the reason for the low number of computer crime prosecutions, it is evident that the current difficulty countries around the world experience in prosecuting virus authors needs correcting. It is no longer sufficient for countries to act independently of one another, through legislation, investigation, or otherwise, because the spread of a computer virus is not a crime likely to be contained within one country. An international solution must be proposed and implemented in order to make successful virus author prosecution a reality.

[*156]

IV. Proposed Solutions

Most experts agree that it would be ideal if international cooperation existed to facilitate the apprehension of virus authors. [n157] Because the outbreak of a computer virus is frequently a cross-border incident, only an international or a uniform approach to the problem can expedite the task of bringing offenders to justice. While no consensus exists as to what is the best method, some proposed solutions have surfaced. These solutions include adopting amendments to domestic legislation to better facilitate extradition, implementing a global cyber crime police unit, and building stronger centralized government. Others, however, advocate government deregulation. The Council of Europe's multilateral draft Cyber-Crime Treaty comprises a final proposed solution to increase the apprehension and prosecution of virus authors.

A. Facilitation of Extradition

One way to facilitate extradition is to change a nation's laws to provide for extradition in the absence of a specific treaty being in place. At the domestic level, language could be added to existing extradition laws to afford more guarantees in the extradition of computer criminals. [n158] If the United States inserted such language into existing legislation, it might read: "The offenses defined herein shall be considered extraditable offenses so long as the Requesting State possesses equivalent legislation and the Requesting State agrees to reciprocate when presented with any similar requests made by the government of the United States." [n159] Such a clause allows extradition even in the absence of an extradition treaty or with an enumerative treaty that does not specifically address computer crimes. [n160] It would also allow extradition for crimes, such as the spread of computer viruses, when most countries recognize the act as criminal but differ in opinion as to appropriate levels [*157] of punishment. There is evidence that this concept might work in countries that have already added similar legislative provisions. [n161] If the United States, which currently lacks such language in its extradition laws, followed suit, extradition for computer crimes would immediately be possible with a number of countries. [n162] A U.S. citizen, however, could not be extradited to a nation that did not have equivalent legislation. [n163]

Amending legislation facilitates the prosecution of virus authors, but it does not solve the problem; some computer crimes may still fall outside extradition's reaches. For example, stronger extradition legislation is not helpful where the requesting country views the act in question as criminal, but the requested country does not. [n164] Inconsistencies in the criminalization of particular conduct is especially likely with crimes such as adult pornography and dangerous speech. [n165] It is unlikely that a country would go to the extreme of amending the legislation simply to achieve the narrow result of facilitating extradition in the area of computer viruses. [n166] In addition, simply amending extradition laws may realistically fail due to the depth of the digital divide that exists in today's world. "In a world where 1.2 billion people [*158] live on less than $ 1 a day," [n167] the problems associated with computers and malicious codes are trivial and irrelevant to many countries. [n168]

An alternative way to facilitate extradition is to amend the treaties themselves, both the substantive and procedural sections, to include computer crimes. As previously discussed, most of the older U.S. treaties list specific offenses that are extraditable, rather than use the newer eliminative method. [n169] Practical application of this solution would force lawmakers to consider amending each of the vast number of extradition treaties the United States already has in place. [n170]

Changing existing treaties or legislation to facilitate extradition is theoretically noteworthy. However, the diversity among national laws on computer crimes forewarn that this solution is of little real merit as it would leave open too

many gaps. In sum, "stronger treaties and a uniformity of computer crime laws must evolve before extradition will ever become a truly effective mechanism for permitting apprehension and prosecution of international computer criminals." n171

B. Varying Levels of Cooperation Between Law Enforcement and the Private Sector

Both law enforcement and the private sector have an interest in combating computer crimes. Separately, the ability of law enforcement and the private sector to combat cyber crime is limited. n172 Some believe, however, that a cooperative effort between the two is the most effective way of preventing and apprehending perpetrators of cyber crime. n173 Many organizations and global leaders have voiced the need for the implementation of such a solution. n174

[*159] Former U.S. Attorney General Janet Reno is not alone in believing that "increased cooperation between law enforcement and industry" n175 is the surest way to effectively handle identifying, locating, and punishing cyber criminals. Reno acknowledged the government's shortcomings in technical ability, pointing out that federal agents are quite aware that the increasing complexity of cyber crimes is exceeding the ability of law enforcement agencies to prosecute them. n176 Without assistance from the private sector, government investigators are at a disadvantage. n177

Interpol, "the world's pre-eminent organization supporting the prevention and detection of international crime," n178 made the idea of cooperation between the public and private sector a reality. Interpol worked directly with AtomicTangerine, a consulting "powerhouse," to create an innovative alliance between the private and public sector. n179 Interpol and AtomicTangerine "initiated a special relationship designed to deliver advanced intelligence collected by the law enforcement organization to corporations worldwide." n180 Basically, law enforcement gives to the private sector the technological advancements aimed at protecting computer systems [*160] from outside attacks. The private sector reciprocates by sharing helpful information it gathers, such as user profiles, to government agencies. n181

While voluntary cooperation between the public and private sectors is a practical solution in theory, it may not be plausible on an international scale. For example, many U.S. corporations do not like the idea of cooperating with law enforcement in criminal investigations, fearing that turning over information may breach privacy agreements they have with their customers. n182 These concerns will continue even if the government tightened its regulations and mandated cooperation during computer crime investigations. n183

C. Stronger Governments

Some government efforts do not require help from the private sector to combat computer crime. In fact, several do not believe that public and private sector cooperation is the solution at all. n184 The public sector strongly believes it must recruit individuals that possess the necessary computer skills, whether they are would-be hackers n185 or corporate computer professionals, n186 to use their talents to combat cyber criminals' technological superiority. One example of this [*161] "independent" approach is the new specialist squad based at the multi-agency National High-Tech Crime Unit in London which targets computer criminals who use the Internet to commit crimes across international borders. n187 The specialist unit, to be set up in April 2001, consists of staff drawn from Customs, National Crime Squad, and the National Criminal Intelligence Service. n188 The United Kingdom invested twenty-five million pounds toward implementing the Unit, a squad totaling over eighty "cyber cops" based in regional police forces around England and Wales. n189 The countries that attended the Group of Eight nations (G8) meeting in Berlin in October 2000 discussed cyber crime and reached an agreement to fund "a team dedicated to Internet crime to provide an instant response... ." n190 To compliment this "strategic fight against crime," the British government committed thirty-seven million pounds to fund a National Management Information System (NMIS) for police forces in England and Wales. n191

NMIS will provide the police with a comprehensive information management and analysis tool, "joining-up' data held on the various information technology systems from every force and area of police work. The system will present this

data in a consistent format so the whole range of police business can be easily and reliably compared and analyzed across the country. [n192]

The funding will also be used to help finance an international hotline to exchange information regarding and facilitating investigations of cyber crimes. [n193]

Again, combating cyber crime by acquiring technological specialists to improve the quality of computer investigations is noteworthy in theory, but not practical. [n194] Individuals with specialized abilities are in demand and unlikely to accept positions with government organizations when private corporations are willing to pay them [*162] relatively higher salaries. [n195] Unless government agencies can increase the salaries of such specialists, they will continue to surrender talent to the private sector.

D. Government Deregulation

The solution primarily advanced by the private sector is for government to refrain from regulating computer crimes that cause security breaches, including computer viruses. Only a minority of IT leaders think extensive government involvement is the correct course of action. [n196] Corporate leaders are interested in letting "technology flourish," and prefer that government "apply no more than a light touch" to Internet security issues. [n197]

Those promoting less government regulation focus on the amount of time allocated by legislators to deal with cyber problems such as computer viruses. Many elected officials believe that "the machinery of government should only be deployed to solve problems that the private sector cannot solve on its own," [n198] and some private sectors agree. [n199] One scholar even suggested that allowing government to obviate what private corporations could accomplish through their own security research is almost harmful: forcing legislators to address issues that the private sector can completely take care of itself, diverts the legislators attention from other pressing matters. [n200] Another concern surrounding the criminalization of computer acts is that legislators often misunderstand technology and thus struggle when [*163] developing solutions. [n201] Lawmaking is already a long term process that desperately tries to keep pace with evolving technology. [n202] In short, the slow process of legislation and the quick growth and change of computer crime do not compliment one another.

Opponents of government regulation also argue that individuals should be left to settle their differences via tort actions. Providing remedies in tort for computer virus infections may effectively deter further virus outbreaks. [n203] Since the "wide-spread, non-uniform" damage caused by virus infections is similar to the personal injuries suffered in other mass torts, it may be best handled by class action suits. [n204] Civil suits would target software companies and Internet service providers (ISPs), giving them incentive to upgrade security and better screen the background of their customers. "Because individuals are often judgment proof, software distributors and on-line service providers present more lucrative targets and must adapt their business strategies to offset this increased risk of liability." [n205] Distributors and ISPs who would bear the majority of the liability can protect themselves by acquiring [n206] liability insurance, making a contractual disclaimer, and developing secure computer strategies.

In theory, holding ISPs and software distributors financially liable in civil tort for the millions of dollars in damages caused by viruses is logical, because they are in the best positions to shoulder the financial burden. In addition the ISP through which the perpetrator spreads the virus onto the Internet can eliminate him as a customer immediately and notify all other ISPs of his identity in order to avoid a recurrence. However, assuring that those harmed are reimbursed for their damages focuses more on the aftermath following a virus release and only contributes marginally to deterring the perpetrator if he is judgment-proof. As earlier noted, deterrence is a basic necessity. [n207] Without the threat of prison, little remains to deter judgment-proof criminals. Furthermore, only providing victims a remedy in civil tort [n208] does nothing to bring the culprit to justice in the criminal forum.

[*164] Regardless of whether a victim can recover monetary damages from a virus attack, the problem of prosecuting the virus author is still not addressed. Allowing for a civil remedy in tort is an important feature in

computer law because it provides companies with an incentive to report the attacks. [n209] However, authorities are still at a disadvantage if there are no criminal laws under which to prosecute cyber criminals. The difficulty of prosecution across international borders pervades without the implementation of a uniform solution applicable to all countries around the world.

E. The Council of Europe's Draft Cyber-Crime Treaty

An effort that solves the uniformity problem for any proposed solution to virus crime is currently underway. "Forty-one countries stretching from Iceland to the former Soviet republic of Georgia could be close to approving a treaty that would fight cyber crime." [n210] In response to the growing number of computer viruses, a special committee of the Council of Europe, [n211] consulting with the U.S. Department of Justice, [n212] proposed a convention "to harmonize cyber-crime laws and facilitate international investigations." [n213] The "Draft Convention on Cyber-Crime" (Draft Treaty) includes, among other things, provisions dealing with illegal access and interception of computerized information of any kind, including data and system interference. [n214] Some provisions contained in the draft treaty limit the production, distribution, and possession of the software used by hackers to exploit computer vulnerabilities. [n215] The Treaty, still in its drafting phase, "will be the first ever international treaty to address criminal behavior directed against computer systems, [*165] networks or data and other types of similar misuse," [n216] and may be signed as early as mid-2001. [n217]

1. The Relevant Provisions of the Treaty

The current draft of the Treaty, released on December 22, 2000, "attempts to level the playing field throughout Europe by standardizing computer crime statutes and requiring signatories to cooperate with one another." [n218] For example, the Draft Treaty requires participating nations to make unathorized access [n219] and interference of computer systems or communications [n220] a criminal offense. Others criminalize the production, sale, distribution, or other distribution of devices or computer programs whose primary use is to access, intercept, or interfere with computer systems or communications. [n221] The Draft Treaty also requires signatory nations to hold corporations liable for crimes committed by an employee holding a "leading position," [n222] and requires ISPs to collect data on their subscribers and make available [*166] such data to authorities. [n223] Signatories are also required to cooperate with other jurisdictions to secure evidence [n224] and extradite persons charged with a computer crime. [n225]

2. Supporters of the Treaty

Various global groups, including the G8 and the Council of Europe, believe that treaties are the only way to align countries against cyber criminals. [n226] These entities recognize that treaties create effective law enforcement and are pressing for treaties that address data and computer crimes. [n227] Draft Treaty's call for the regulation of "cyberweapons," such as hacking tools that have generally escaped regulation, has been praised. [n228] "Cyberweapons control would establish a standard for behavior on the Internet and provide a means for prosecuting offenders. Their enforcement could curtail attacks and limit the damage by those brazen enough to violate the law." [n229]

[*167] The Draft Treaty eliminates many of the problems found with the other proposed solutions previously discussed. [n230] For instance, the need to change domestic legislation [n231] or amend existing treaties [n232] in order to facilitate extradition becomes irrelevant because the Draft Treaty contains provisions that ameliorate the dilemma. [n233] The problem of facilitating cooperation between the public and private sectors during criminal investigations is also solved by provisions in the treaty making such cooperation mandatory for all signatories. [n234] The same provision also eliminates the complications involved in strengthening government agencies by increasing the number of highly skilled technical investigators [n235] because all involved work cooperatively. [n236] In sum, the Draft Treaty surpasses the other proposed solutions by resolving the prosecutorial problem in one effort as opposed to a combination of many.

3. Opposition

Outright support is not the only response that the Council of Europe's Draft Treaty received. Some have protested the Draft Treaty, arguing that this recent attempt to remedy the inability of countries to effectively prosecute virus authors leaves open too many gaps. [n237] The opposition asserts that provisions may be over-broad, thereby inadvertently over-regulating security software currently available on the commercial market. [n238] Private companies are anxious because the Draft Treaty contains what they consider burdensome mandates on ISPs to save and possibly relinquish information regarding their customers. [n239] Tension also surrounds the controversial assistance of the United States in the Treaty's drafting. [n240]

"European Union nations ... are about to make nearly any form of hacking - even security research - illegal by treaty." [n241] Members of the private sector voiced strong opposition to the Treaty. [n242] Currently, hacking for security research purposes is legal in the United States. [n243] Professional network administrators fear the Draft [*168] Treaty may chill security research. [n244] It is necessary to discover possible security breaches and alert others of potential dangers. [n245] For the most part, the computer software used to accomplish this type of research has the potential to be used for illegal hacking. [n246] Some are concerned that the language in the current version of the Draft Treaty may lead some countries to construe simple possession of such software as intent of malicious activity. [n247]

Additionally, opponents are outraged that the Draft Treaty requires "internet service providers and network administrators to help police by maintaining detailed logs of all network activity," [n248] a measure that at least one U.S. statesman bluntly denounced. [n249] Some U.S. Senators repeatedly refuse to support any domestic legislation that requires private sectors to cooperate with the government, [n250] an intentional goal of the Draft Treaty. One senator "cautioned security managers that the federal government does not have adequate resources to prosecute security attacks," and urged Congress not to pass legislation that forces companies to cooperate with investigations. [n251]

[*169] Civil rights activists share the private sector's concerns regarding the Draft Treaty [n252] and additionally accuse the United States of improperly using its global influence. [n253] The Global Internet Liberty Campaign (GILC), [n254] a civil rights coalition of twenty-eight international cyber-rights organizations, opposes the European Union's Draft Treaty on Cyber-Crime. [n255] Specifically, the GILC takes issue with the involvement of members of the U.S. Department of Justice and Federal Bureau of Investigation in the Treaty's drafting. [n256] "[GILC] members believe that U.S. law enforcement is attempting to gain international support for modifications to its own country's laws - support that it has not been able to gain domestically." [n257] The GILC fears that, once a significant amount of European countries signed the Treaty and argue that the United States must "reconcile its laws with - what then will have become - the international norm," U.S. Treaty supporters could bring the agreement back to Congress. [n258] The GILC campaign interprets U.S. tactics as an "endrun" approach to gain the support overseas for an expansion of authority because it cannot acquire the support domestically. [n259]

[*170]

V. Conclusion

A successful cyber crime treaty must address three major areas in order to effectively bring about much needed prosecutions: recognition and enforcement of criminal judgments issued by a particular country's court, efficient and expedient cooperation between nations in the retention of evidence and witnesses, and consistent extradition of criminals. [n260] In light of the vast number of computer crimes occurring today, virus regulation and prosecution comprise the most efficient subject matter for a treaty because they involve an area of computer crime that all countries agree must be criminalized. [n261]

In approaching any long term goal, the drafters of the Treaty must address how much attention a country is willing to devote to computers and Internet problems "in a world where 1.2 billion people live on less than $ 1 a day." [n262] This issue inevitably goes hand in hand with the need to measure the depth of the globe's digital divide and devise strategies for closing high tech gaps in order to ensure that the Internet is built as an "Internet for all as opposed ... to an Internet for a few." [n263]

The Council of Europe's Draft Cyber-Crime Treaty provides the best framework for a successful international solution, a solution with the potential to bring results. As currently drafted, [n264] the Draft Treaty's biggest potential problem is that the language may inadvertently result in criminalizing techniques and software commonly used to aid many computer systems in resisting attack. [n265] This may result in a chilling effect on research and the use of many types of security tools. [n266]

The Draft Treaty is scheduled to be signed into effect in June 2001, but there still remains a number of interpretation problems within its language. By proceeding with caution and taking care to address all valid concerns, the Council of Europe can avoid hasty lawmaking that could do more harm than good. If given the time it needs to adequately develop, this Draft Treaty has the potential to offer the international solution necessary to successfully prosecute computer virus authors.

Legal Topics:

For related research and practice materials, see the following legal topics:
Computer & Internet LawCriminal OffensesSoftware CrimesComputer & Internet LawCriminal OffensesData Crimes & FraudComputer & Internet LawCriminal OffensesComputer Fraud & Abuse Act

FOOTNOTES:

n1. A large portion of corporate computer systems are misused or sabotaged by corporate employees. See *United States v. Sablan, 92 F.3d 865, 866 (9th Cir. 1996)* (affirming the conviction of a former bank employee who logged into the bank's computer system with her old password and damaged files); see also Jonathan Saltzman, Computer Expert Faces Charge of Putting Virus in Textron's System, Providence J. Bull., Oct. 1, 1996, at A1, available at *1996 WL 12467001* (reporting authorities' description of a computer specialist accused of causing damage to Textron's computers by e-mailing programs infected with a virus to all Textron's computer system users as a "disgruntled employee"); see Martin Wolk, Danger on the Home Front, MSNBC, (Oct. 31, 2000), at http://www.msnbc.com/news/483684.asp (copy on file with The Transnational Lawyer) (discussing how often the culprit of a security breach in a corporation is one of the corporation's own employees); see David Noack, Employees, Not Hackers, Greatest Computer Threat, MSNBC (Jan. 4, 2000), at http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104 01.html (copy on file with The Transnational Lawyer). Teenagers are also common culprits responsible for virus epidemics. See Leef Smith, Web Marauder Pleads Guilty; U.S. Government Sites Were Among Targets of "Zyklon,' Wash. Post, Sept. 8, 1999, at B2.

n2. The term "code" is defined as "instructions written in a computer programming language." Webster's New World Dictionary of Computer Terms 110 (8th ed. 2000) [hereinafter Webster's Dictionary].

n3. An "infection" of a computer is defined as "the presence of a virus within a computer system or on a disk. The infection may not be obvious to the user; many viruses, for example, remain in the background until a specific time and date, when they display prank messages or erase data." Id. at 275.

n4. The term "dial-up modem" is defined as follows: "In contrast to a modem designed for use with a leased line, a modem that can dial a telephone number, establish a connection, and close the connection when it is no longer needed. Most personal computer modems are dial-up modems." Id. at 160.

n5. A "dial-up access" is defined as "a means of connecting to another computer or a network such as the Internet with a modem-equipped computer." Id. at 159.

n6. An "e-mail" is defined as "the use of a computer network to send and receive messages. Also called electronic mail. Although transmission is instantaneous or nearly so, the message may not be received until the recipient logs on and receives notice that mail has arrived." Id. at 186.

n7. See Eric J. Sinrod & William P. Reilly, Cyber-Crimes, A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer & High Tech. L.J. 177, 216 (2000) (noting that a malicious code can also be transmitted via an infected computer disk).

n8. See *Reno v. A.C.L.U., 521 U.S. 844, 851(1997)* (discussing the history and background of the Internet).

n9. A "virus" is defined as

a program designed as a prank or as sabotage that replicates itself by attaching to other programs and carrying out unwanted and sometimes damaging operations. When viruses appear, the effects vary, ranging from prank messages to erratic system software performance or catastrophic erasure of all the information on a hard disk. Don't ever assume that a prank message means that's all the virus will do.

Webster's Dictionary, supra note 2, at 563.

n10. See infra notes 101-05 and accompanying text (setting forth how the outbreak of the Chernobyl virus posed this particular prosecutorial problem for Taiwan).

n11. See infra notes 108-13 and accompanying text (setting forth how the outbreak of the ILOVEYOU virus posed this particular prosecutorial problem for the Philippines).

n12. See John T. Soma et al., Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?, 34 Harv. J. on Legis. 317, 318 (1997) (explaining that "the process of extradition can be defined simply as the surrendering of a criminal or accused criminal by one sovereign to another"); see also I.A. Shearer, Extradition in International Law 5 (1971); see also M. Cherif Bassiouni, International Extradition and World Public Order 1 (1974) (providing a complete discussion on extradition).

n13. See infra note 155 and accompanying text (illustrating the wide discrepancy in prison sentences for computer offenses in various countries).

n14. See Joshua Dressler, Cases and Materials on Criminal Law 29-77 (2d ed. 1999) (discussing the theories of deterring punishment and relevant U.S. case law).

n15. The phrase "virus author" is used in a broad sense throughout this Comment. It defines an individual who intentionally causes a malicious code to reach the Internet, whether injected directly or indirectly, and is not limited to merely the individual who wrote the code.

n16. See infra notes 23-41 and accompanying text (detailing the mechanics of a computer virus).

n17. See, e.g., infra notes 101-13 and accompanying text (discussing how the authors of the ILOVEYOU and Chernobyl viruses managed to escape prosecution because the Philippines and Taiwan did not have cyber crime legislation in place at the time the acts were committed).

n18. " Cyber " is defined as "a prefix that means computer." Webster's Dictionary, supra note 2, at 139.

n19. The Draft Cyber-Crime Treaty is currently being drafted and reviewed by the Council of Europe and is the latest attempt to fight cyber crime. For a complete discussion on the Council of Europe's Draft Cyber-Crime Treaty within the context of this Comment, see infra notes 210-59 and accompanying text.

n20. See infra notes 23-41 and accompanying text (expounding a detailed description of the basics of a computer virus and what it constitutes).

n21. See infra notes 42-53 and accompanying text (specifying how spreading a strand of malicious code can constitute a criminal act).

n22. See infra notes 54-78 and accompanying text (giving examples of three infamous virus authors and the havoc they have wreaked).

n23. See Sinrod & Rielly, supra note 7, at 215-23 (explaining that other types of malicious codes include worms and Trojan Horse programs).

Worms are similar to viruses. However, one major distinction is that worms multiply without any human interaction. A worm can wind its way through a network system without the need to be attached to a file, unlike viruses... . [A] Trojan Horse program, or Trojan program, is an innocent-looking program that contains hidden functions. They are loaded onto the computer's hard drive and executed along with the regular program. However, hidden in the belly of the "innocent' program is a sub-program that will perform a function, mostly unknown to the user. Trojan programs can take the form of a popular program where the original source code had been altered to hide the Trojan "payload.'

Id. at 223.

n24. Id. at 215.

n25. Id. at 216.

n26. Id. (describing how not all viruses do damage to their hosts). "For example, a virus could display an innocuous message on a certain date. Although it might be annoying and create a sense of anxiousness, the virus does not cause any measurable harm." Id.

n27. Id.

n28. Id. (distinguishing a virus that needs to be executed in order to infect a computer from a worm, which does not require human interaction to infect a host computer). In order to "execute" a virus or a program, the computer user must somehow activate it manually, usually by opening an attachment or running a program. Id. But see Symantec, VBS.BubbleBoy, at http://www.symantec.com (visited Feb. 17, 2001) (copy on file with The Transnational Lawyer) (describing how the BubbleBoy virus, which works under Windows 98 and Windows 2000, activates when the infected e-mail is viewed and does not require detaching and running an attachment).

n29. See Sinrod & Rielly, supra note 7, at 216.

n30. A "macro" is defined as "a program consisting of recorded keystrokes and an application's command language that, when run within an application, executes the keystrokes and commands to accomplish a task. Macros can automate tedious and often-repeated tasks, such as saving and backing up a file to a floppy, or can create special menus to speed data entry." Webster's Dictionary, supra note 2, at 331.

n31. See Sinrod & Rielly, supra note 7, at 217.

n32. An "executable program" is defined as "a program that is ready to run on a given computer. For a program to be executable, it first must be translated, usually by a compiler, into the machine language of a particular computer." Webster's Dictionary, supra note 2, at 197.

n33. See supra note 30 (defining a "macro").

n34. Sinrod & Rielly, supra note 7, at 217.

n35. Id.

n36. Id. at 217 n.176 (explaining that the virus can be programmed by the author to trigger on a certain date, when the computer user enters

a certain word, when the computer restarts, after a certain amount of time has passed after the virus is loaded into the system, or in any number of creative ways).

n37. Id. (explaining how a virus can hide in the computer's memory or in the computer programs so that it is activated each time the program is loaded).

n38. Id. at 216.

n39. Id. at 217.

n40. Id. at 217 n.185 (illustrating the interactive relationship between the hard drive, processor, RAM, and operating system). The following excerpt offers a general description of how the process works:

A hard disk, or memory, is the main memory where the programs and the operating system are permanently stored. As an example, one can think of the hard drive as a large filing cabinet, the random access memory (RAM) as a table, and the processor as a clerk. When the clerk wants to work on a file, he goes to the filing cabinet and brings the file to the table, where he can open up the file and read it. If the clerk wants to read another file, he repeats the process. The relationship between the hard drive, RAM, and processor can be further illustrated by adjusting the variables. If a lot more filing cabinets are added, but the size of the desk is still the same, the clerk will not be able to increase the number of files he can put on the table. If the size of the desk is increased, but the clerk moves slowly, then too many files on the desk may actually slow him down. The operating system is the set of instructions that coordinate all of the actions that take place in the computer. Although operating systems often come on CD-ROMs, they are not "computer programs." A program can only run "on top of an operating system." The operating system is like the translator that gets all of the hardware and software talking together. In the above example, the operating system is like the employee handbook that tells the clerk what he is supposed to do and how he is supposed to do it.

Id.

n41. Id. at 218 (noting one recent example of an irritating, yet harmless virus: "W95.LoveSong.998," which caused a Korean love song to play on a certain date). "The Emperor" is an example of a devastating virus. Id. It will "permanently overwrite data on the hard disk and then attempt to destroy the Flash BIOS (basic input-output system)." Id.

n42. See infra note 46 (considering crimes other than the spread of computer viruses that qualify as computer crimes).

n43. See, e.g., the Counterfeit Access Device and Computer Fraud and Abuse Law, Pub. L. No. 98-473, 2102(a), 98 Stat. 1837, 2190 (1984) (enacting the first computer crime legislation in the United States in 1984).

n44. See infra note 92 and accompanying text (explaining that the current version of *18 U.S.C. 1030* requires only an intent to access, not an intent to cause damage).

n45. See, e.g., Sinrod & Rielly, supra note 7, at 179 (discussing traditional crimes of money laundering and child pornography that become computer crimes when a computer is used to facilitate the act).

n46. The spread of a computer virus is one example of a crime that qualifies as a computer crime because the computer itself is the target of the offense. See id. at 187 (discussing other ways that a crime can qualify as a computer crime: when a computer merely contains the evidence that a crime was indeed committed, and when a computer is the tool used to commit the offense). An example of the former is a money launderer who "may use a computer to store details of his laundering operation instead of relying on paper accounting records." Id. Another example includes child pornographers whose "computers are often seized as the key evidence that the defendant produced, possessed, received, and/or distributed child pornography." Id.; see also Veronica C. Silva & Pauline Anne P. Escalante, Vigilance the Only Sure Solution to Cybercrimes (First of Two Parts), Bus. World (Philippines), May 9, 2000, at 16, available at *2000 WL 18794738* (explaining that an example of the latter, a crime where the computer is the tool used to commit the crime, is a Denial of Service (DoS) attack). "DoS is not a virus but it prevents internet traffic from reaching the target websites. The attacker in this case bombards the target sites with millions of messages, thus preventing bonafide [sic] users from accessing these for hours." Id.

n47. See Sinrod & Rielly, supra note 7, at 180 (explaining how "current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy"); see generally, Silva & Escalante, supra note 46, at 16.

n48. See Silva & Escalante, supra note 46, at 16 (stating the opinion of Ramon Ike V. Seneres, Director-General of the National Computer Center in the Philippines, that the offense should be prosecuted as merely an extension of traditional crimes). "There is no need to create special laws to prosecute cybercrimes if there are existing implementable laws." Id. Hacking, he said, is merely breaking and entering, and "if you take something then there's theft. The computer or the Internet is just a medium like PayTV, magazine, or VHS." Id.; Allen R. Stein, The Unexpected Problem of Jurisdiction in Cyberspace, Symposium on Jurisdiction and the Internet, *32 Int'l Law. 1167, 1167 (1998)* (opining that Internet activity "does not challenge existing jurisdictional paradigms"). "There is nothing about legal relations over computer networks that in any way challenges our conventional notions about how sovereign authority is allocated in the world." Id.; see generally, Tomas A. Lipinski, The Developing Legal Infrastructure and the Globalization of Information: Constructing a Framework for Critical Choices in the New Millennium Internet - Character, Content and Confusion, *6 Richmond J. L. & Tech. 19* (1999-2000) (discussing the extension of traditional property rights and other information controls and regulations into cyberspace).

n49. See Laura J. Nicholson et al., Computer Crimes, *37 Am. Crim. L. Rev. 207, 212 (2000)* (describing how these include jurisdiction, international cooperation, intent, and the difficulty of identifying the perpetrator).

n50. While state computer crime statutes do exist, this Comment only considers relevant federal statutes.

n51. *18 U.S.C. 1030* (2000); see also infra notes 87-92 and accompanying text (discussing the National Information Infrastructure Protection Act).

n52. See Nicholson, supra note 49, at 220-22. For example, if the crime committed is a copyright violation, a computer software company whose product is being replicated might choose to prosecute under the Copyright Infringement Act, *17 U.S.C. 506* because it is relatively easy to establish the elements of the crime: the unauthorized copying of computer software, done willfully, for financial or commercial gain, or in the alternative reproduction or distribution of software of a certain market value, without regard to financial gain. Id.

n53. See infra notes 120-28 and accompanying text (discussing the problems surrounding prosecution even when a tailor-made statute is in place).

n54. See, e.g., Bob Sullivan, MSNBC, Virus Won't Let Victims Get Help (Nov. 28, 2000), at http://www.msnbc.com/news/495873.asp (copy on file with The Transnational Lawyer) (describing a computer virus "smart enough to block its victims from getting help"). "The bug, called MXT, was discovered in August [of 2000] ... [and] has one very sinister feature: once it infects a user, it's programmed to stop the victim from visiting antivirus Web sites and sending "mayday" e-mails to antivirus companies." Id.

n55. See infra notes 244-47 and accompanying text (voicing the concern of those opposed to any government regulation that would hinder this type of security research).

n56. See, supra note 1 and accompanying text (citing a few examples of security breaches caused by corporate employees); see also Jack McCarthy, Hacker Mitnick Could Be Released by Early 2000, InfoWorld Daily News, Aug. 10, 1999 , available at LEXIS, News Library, INFDLY File (describing sentencing and charges against Kevin Mitnick, an infamous hacker who broke into computer networks and stole credit card numbers and software). "Investigators arrested Mitnick in 1995 following a well-publicized manhunt that was the subject of the book entitled "Takedown.' He was charged with 25 counts of wire and computer fraud for breaking into the networks of companies, including Sun Microsystems, Novell, and Motorola." Id.

n57. See Sinrod & Rielly, supra note 7, at 215 (citing a report compiled in the United States by the Computer Emergency Response Team (CERT) estimating that 30,000 computer viruses currently exist and that approximately 300 new viruses are created each month).

n58. See Dressler, supra note 14, at 1-6 (discussing the nature, sources, and limits of the criminal law).

n59. See Damien Whitworh & Dominic Kennedy, Author Could Escape Arm of the Law, Times (London), May 5, 2000 (estimating the amount of fiscal damage caused by the Melissa virus in 1999).

n60. See Andrew J. Glass, Number, Types of Viruses Promise Only to Increase, San Diego-Union Trib., Jun. 22, 1999, at 4, available at LEXIS, News Library, SDUT File.

n61. See The Year's Computer Diseases, San Diego Union-Trib., June 22, 1999, at 4, available at LEXIS, News Library, SDUT File.

n62. See Sinrod & Rielly, supra note 7, at 218 (describing the manner in which the Melissa virus perpetuated).

The Melissa Macro Virus was a virus that was hidden in a Microsoft Word attachment that appeared to come from a person known to the recipient. When the attachment was opened, a list of pornographic web site passwords were displayed. However, unknown to the user, the program also activated a macro that read the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses... .

Id.

n63. See id. (recounting that one company reported that its "500-employee computer network was buffeted by 32,000 e-mail messages in a 45 minute period, effectively shutting it down for legitimate purposes").

n64. Meltdown of the Different Kind, Computimes (Malaysia), May 3, 1999.

n65. See id. (explaining that the virus name of "CIH" represents the initials of its author, Chen Ing-hau). Ing-hau developed the virus when he was an engineering student at Taiwan's Tatung Institute of Technology. Id.

n66. See Whitworth & Kennedy, supra note 58.

n67. Ann Harrison, Chernobyl Virus Not Even a Cold for Most U.S. Companies, Computerworld, May 3, 1999, available at LEXIS, News Library, CMPWLD File; see also The Year's Computer Diseases, supra note 60, at 4 (describing how the Chernobyl virus spread itself from computer to computer).

n68. Taiwan Prosecutes Chernobyl Virus Inventor, Deutsche Presse-Agentur, Sept. 11, 2000, available at LEXIS, News Library, DPA File [hereinafter Taiwan Prosecutes].

n69. See Harrison, supra note 67, at 4 (stating that the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University in Pittsburgh found that only 2,328 computers in the United States reported damage by the virus). ""Most of the reported victims were home computer users and university students and faculty', said CERT spokesman Bill Pollak. "By contrast, 100,000 computers were infected with the Melissa virus,' CERT said." Id.

n70. See id. (elaborating on how the United States improved its virus defense abilities after fighting off the Melissa virus attacks earlier in the year). ""The main reason most U.S. businesses were spared was that the Melissa virus and its notoriety inspired companies to update or actually purchase antivirus software,' said Sal Viveros, marketing manager at Network Associates Inc. in Santa Clara, Calif." Id.

n71. Id.

n72. See id. (describing the widespread destruction in other countries caused by Chernobyl). "The Chernobyl virus damaged at least 700,000 computers in the Middle East and Asia. In South Korea, the virus infected over 250,000 computers. The virus also damaged about 100,000 PCs in China and 300,000 in Turkey... ." Id.

n73. See "Love Bug' Sparks Demand for Internet Policy Changes, Asia Pulse, May 8, 2000, available at *2000 WL 2694811* [hereinafter "Love Bug' Sparks Demand].

n74. Id.

n75. Editorial, Computer Viruses Pose Global Threat, Yomiuri Shimbun/Daily Yomiuri, May 9, 2000, available at *2000 WL 20279161*.

n76. Id.

n77. Silva & Escalante, supra note 46, at 16.

n78. India: The Virus of Cyber-Crimes, Bus. Line (Hindu), May 31, 2000, available at *2000 WL 19063708* [hereinafter India].

n79. Nicholson, supra note 49, at 250.

n80. See infra notes 101-13 and accompanying text (illustrating how two virus authors caused extensive damage around the world yet evaded prosecution because the country where they were found did not have an adequate law under which to prosecute them; these countries became "havens" of safety from the arm of the law).

n81. See Nicholson, supra note 49, at 220-31 (discussing other federal statutes aside from the National Information Infrastructure Protection Act under which a computer crime may be prosecuted; these include, but are not limited to, the Copyright Act, the National Stolen Property Act, the mail and wire fraud statutes, the Electronic Communications Privacy Act, the Communications Decency Act of 1996, and the Child Pornography Prevention Act of 1996).

n82. See United States Sentencing Commission, Computer Fraud Working Group, Report Summary of Findings 3 (1993) (surmising that even though traditional statutes are capable of prosecuting some computer crimes, those crimes that are specialized computer offenses need more specifically tailored laws of their own).

n83. In 1984, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Law. Pub. L. No. 98-473, 2102(a), 98 Stat. 1837, 2190 (1984) (current version at *18 U.S.C. 1030* (2000)).

n84. Congress revised its 1984 legislation three times in 1986, 1988, and 1989. For past versions of *18 U.S.C. 1030*, see respectively, Pub. L. No. 99-474, 2, 100 Stat. 1213 (1986) (current version at *18 U.S.C. 1030* (2000)); Pub. L. No. 100-690, 7065, 102 Stat. 4404 (1988) (current version at *18 U.S.C. 1030* (2000)); Pub. L. No. 101-73, 962(a)(5), 103 Stat. 503 (1989) (current version at *18 U.S.C. 1030* (2000)).

n85. Congress revised its legislation three more times during the 1990s in 1990, 1994, and 1996. For past versions of *18 U.S.C. 1030* for each corresponding version, see respectively, Pub. L. No. 101-647, 1205(e), 2597 (j), 3533, 104 Stat. 4831, 4910, 4925 (1990) (current version at *18 U.S.C. 1030* (2000)); Pub. L. No. 103-322, 290001(b)-(f), 108 Stat. 2097-2099 (1994) (current version at *18 U.S.C. 1030* (2000)); Pub. L. No. 104-294, 201, 110 Stat. 3488, 3491-94 (1996) (current version at *18 U.S.C. 1030* (2000)).

n86. See Nicholson, supra note 49, at 212 (explaining that the volume of the original legislation of the 1984 Counterfeit Access Device and Computer Fraud and Abuse Law expanded greatly to address the growing number and types of computer-related crimes in existence).

n87. See supra notes 83-85 (tracing the changes that Congress has made through the years to the Counterfeit Access Device and Computer Fraud and Abuse Law).

n88. Id. at 212 (tracing the changes that Congress has made through the years on the legislation as new criminal issues involving computers have arisen).

The 1984 Act was intentionally narrowly tailored to protect classified United States' defense and foreign relations information, financial institution and consumer reporting agency files, and access to computers operated for the government... . In the Computer Fraud and Abuse Act of 1986, Congress expanded the scope of the law and attempted to define its terms more clearly. Congress continued to expand the scope of the computer crime law ... and then passed the National Information Infrastructure Protection Act of 1996 (NIIPA) ... One important change effectuated by the 1996 Act was the substitution of the term "protected computers," for "federal interest computers," throughout the statute. Previously, the 1994 Act only covered crimes involving computers located in more than one state. Because "protected computers" includes those used in interstate commerce or communications, the statute now protects any computer attached to the Internet, even if all the

computers involved are located in one state.

Id.

n89. See *18 U.S.C. 1030*(e)(8)(A)-(D) (2000)."Damage" is defined as follows:

(8) any impairment to the integrity or availability of data, a program, a system, or information, that

(A) causes loss aggregating at least $ 5,000 in value during any one year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety... .

Id.

n90. " The term "exceeds authorized access' means access to a computer without authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." *18 U.S.C. 1030*(e)(6).

n91. Nicholson, supra note 49, at 215.

n92. See id. at 216-17 (explaining how the prior versions of the 1996 Act did not technically criminalize accessing a private sector, non-financial computer for the purpose of fraud from within the same state, due to loopholes created by the language). The 1996 Act also removed available defenses regarding intent. Id. at 217.

Section 1030(a)(5)(C) now clearly requires only an intent to access, not an intent to cause damage. Even under the 1986 Act, the language was judicially interpreted by the Second Circuit in *United States v. Morris, 928 F.2d 504 (2d Cir. 1991),* as requiring intent merely to access, not intent to cause damage. The Ninth Circuit also held that the lack of a mens rea requirement for causing damage was constitutional. Thus, once a prosecutor proves intentional access, courts will reject a defense claiming that the effects of a program exceeded the programmer's intentions.

Id.; see also Sinrod & Reilly, supra note 7, at 220 (discussing new changes to federal cyber crime statues with regard to the element of intent). A prosecutor is no longer required to prove a culprit's intent to harm; now a prosecutor must only prove intent to access files in an unauthorized way. Id.

n93. Sinrod & Reilly, supra note 7, at 219.

n94. See Whitworth & Kennedy, supra note 57 (reporting that a combination of amateur sleuths, investigators from the Federal Bureau of Investigation, and major Internet companies took part in "hunting" the culprit).

n95. See Sinrod & Rielly, supra note 7, at 219 n.192 (reporting that Mr. Smith pled guilty to second-degree computer theft under N.J.S.A. 2C:20-25).

n96. See id. at 219 (citing *18 U.S.C. 1030*(a)(2), (5)(A) (2000) as the applicable federal statute under which Smith pled guilty).

n97. Id.

n98. As of the time of this Comment's publication, Smith had not yet been sentenced.

n99. See Jo Ticehurst, 7 Days; Cybercrime is Unpunished, Computing, Dec. 14, 2000, at 6, available at LEXIS, News Library, COMPTG File (espousing the fear that "new kinds of crimes can fall between the cracks," causing many cyber crimes to go unpunished in many countries due to gaps in national criminal laws).

n100. See Whitworth & Kennedy, supra note 58.

n101. See Sylvia Dennis, Chernobyl Virus Author Arrested in Taiwan, Newsbytes, Sept. 18, 2000. "He subsequently won a job at a software company on the back of his infamy." Id.; see also Whitworth & Kennedy, supra note 59 (explaining that Ing-hau's infamous virus actually brought him acclaim in Taiwan). ""He is treated as a national hero,' Jan Hruska, technical director of Sophos, the anti-virus specialists of Abingdon, Oxfordshire, said." Id.

n102. See Taiwan Prosecutes, supra note 68 (describing how a Taiwan resident was prompted to file criminal charges against Ing-hau when the virus struck again on April 26, 2000 and his personal computer was infected).

n103. Dennis, supra note 101.

n104. Taiwan Prosecutes, supra note 68.

n105. See id.

n106. See, e.g., supra notes 88-92 and accompanying text (describing NIIPA, the U.S. law that is specifically designed to combat computer crime).

n107. See supra note 102.

n108. See Philippines: "Love Bug' Suspect Gets Off the Hook, Computerworld Philippines, Aug. 28, 2000, available at *2000 WL 9787658* [hereinafter Philippines: "Love Bug'] (naming Onel de Guzman as the suspected author of the Love Bug). At the time of the incident, de Guzman was a 23-year-old computer student of AMA Computer College. Id.

n109. See Luz Baguioro, Philippines Indicts "Love Bug' Suspect, Straits Times (Singapore), June 30, 2000, available at *2000 WL 2978251* (naming the National Bureau of Investigation and a local Internet service provider as the organizations that brought the formal charges against de Guzman).

n110. " Love Bug" Sparks Demand, supra note 73.

n111. See Philippines: "Love Bug,' supra note 108 (confirming that the Department of Justice of the Philippines cleared de Guzman of all charges in a resolution approved by Chief State Prosecutor Jovencito Zuno in late August 2000).

n112. Id.

n113. See id. (quoting Archimedes Manabat, one of the member-prosecutors of the three-man Department of Justice panel that reviewed the case as stating that the "e-commerce law cannot be enforced because it was ratified after the hacking was done").

n114. See Melvin G. Calimag, 5 Asian Countries Now Have E-Commerce Laws, Metropolitan Computer Times, June 15, 2000 (reporting that the Electronic Commerce Act of 2000 is based on the Model Law on Electronic Commerce, drafted by the United Nations Commission for International Trade Law (UNICITRAL)). The article also quoted Guillermo Luz of the Makati Business Club: "We're surprised, but happy. I think the House of Representatives did an extraordinary thing of passing the bill in the 2nd and 3rd reading on the same day." Id. A complete copy of the Electronic Commerce Act of 2000 is on file with The Transnational Lawyer; see also Philippines: New Law Paves Way For E-Transactions, Computerworld Philippines, June 30, 2000, available at *2000 WL 9787565* (marveling at how, just two years after it was conceptualized, "both the Senate and the House of Representatives ratified the bicameral conference committee report on the proposed E-Commerce Act, all within June 2000, barely making it before the closing of the second regular session of the 11th Congress").

n115. See Luz Baguioro, Philippines Approves Bill on Cyber-Crimes, Straits Times (Singapore), June 9, 2000, available at *2000 WL 2975454* (outlining the fine and jail terms provided by the Electronic Commerce Act for computer hacking and other cyber attacks). "The Bill ... aims to plug the hole that hampered Manila's efforts to prosecute those suspected of creating and spreading the Love Bug computer virus." Id.; see also Philippine President Signs E-Commerce Law, Deutsche Presse-Agentur, June 14, 2000 (quoting President Joseph Estrada as saying that "it is indeed unfortunate that the country's good name suffered unfairly in the wake of the infamous ILOVEYOU virus. This law provides fines and penalties for computer hackers - a three year imprisonment and a minimum fine of 100,000 pesos (2,400 dollars)." Id.

n116. See supra notes 101-13 and accompanying text (illustrating how Taiwan and the Philippines became "havens" for two virus authors who evaded prosecution because the country authorities found them and did not have adequate cyber crime laws).

n117. This is only when countries have not resorted to international cooperation.

n118. Nicholson, supra note 49, at 250; see also *Reno v. A.C.L.U., 521 U.S. 844, 851 (1997)* (defining cyberspace as a "unique medium ... located in no particular geographic location but available to anyone, anywhere in the world, with access to the Internet").

n119. See supra notes 59-78 and accompanying text (discussing the outbreaks of the computer viruses Melissa, Chernobyl, and ILOVEYOU). This Comment addresses Internet virus outbreaks occurring only between the dates of 1999 and 2000. For discussion surrounding viruses occurring in 2001, see Bob Sullivan, MSNBC, Melissa Variant Targets Macintosh (Jan. 18, 2001), at http://www.msnbc.com/news/518157.asp (copy on file with The Transnational Lawyer) (reporting a new strain of the Melissa virus specifically targeting Macintosh computers). "The new virus is tricky because it attacks Microsoft Word 2001 for Macintosh files, a new file format many antivirus products can't quite handle yet." Id.; MSNBC, Password-Stealing Virus Hits AOL (Feb. 1, 2001), at http://www.msnbc.com (copy on file with The Transnational Lawyer) (reporting the revival of an old virus that has been given "new life"). "The strand that is currently making the rounds spreads through AOL e-mail and infects files on users' systems while attempting to collect and steal AOL v4.0 and v5.0 account numbers and passwords." Id.; Bob Sullivan, MSNBC, Italian "Love Bug' Hits Euro Firms, (Feb. 8, 2001), at http://www.msnbc.com/news/527791.asp (copy on file with The Transnational Lawyer) (reporting a new Italian version of the "Love Bug" is hitting companies in Europe); Robert Lemos, MSNBC, Dutch Arrest "Kournikova' Suspect (Feb. 14, 2001), at http://www.msnbc.com/news/529834.asp (copy on file with The Transnational Lawyer) (reporting that Dutch police "arrested and released a man who confessed responsibility for writing the Anna Kournikova virus that inconvenienced thousands of Internet users"). The charges against the 20 year-old suspected author for damaging private property and computer programs were insufficient to keep him incarcerated. Id. "The virus itself is relatively benign; its payload executes only once a year, on Jan. 26, when it redirects victims' Internet browsers to a Web page in the Netherlands. But because it makes so many copies of itself, it can shut down corporate e-mail servers." Id.

n120. See Nicholson, supra note 49, at 231 (discussing how unsuccessful the United States has been in bringing cyber criminals to justice).

The unamended version of the 1984 Computer Abuse Act resulted in only one prosecution. Between January 1989 and April 1993, there were only seventy-six convictions under *18 U.S.C. 1030.* A study of fifty such cases revealed that more than half were convictions for general fraud under 1030(a)(4). The number of such prosecutions reached 174 as of June 1996.

Id.

n121. See id. (discussing how the restriction of the Computer Fraud and Abuse Act to actions affecting "federal interest computers" could have influenced the low number of prosecutions).

One important change effectuated by the 1996 Act was the substitution of the term "protected computers," for "federal interest computers," throughout the statute. Previously, the 1994 Act only covered crimes involving computers located in more than one state. Because "protected computers" includes those used in interstate commerce or communications, the statute now protects any computer attached to the Internet, even if all the computers involved are located in one state.

Id.

n122. See Carl Benson et al., Computer Crimes, *32 Am. Crim. L. Rev. 409, 422 (1997)* (asserting that the vulnerability of its computer systems to the public often deters private corporations from reporting security breaches). "Owners ... may prefer to handle security problems themselves to avoid the embarrassment of a public trial focusing on the vulnerability of their computers." Id.

n123. See India, supra note 78 (intimating that the most difficult challenge is identifying the culprit). "As the Net can be accessed from any part of the globe, the field is wide open for hackers. At present, there are an estimated 198 million Net connections." Id.; see also Bruce Braun et al., WWW.Commerical Terrorism.com: A Proposed Federal Criminal Statute Addressing the Solicitation of Commercial Terrorism Through the Internet, 37 Harv. J. on Legis. 159, 175 (2000) (discussing how anonymity on the web is still relatively easy to maintain). For example, logging on to a computer from a cyber cafe or library can make it almost impossible for police to track down a culprit who uses such a public terminal for criminal activity. Id. For most Internet connections, because users need not provide identification to log on, investigators encounter additional tracking difficulties. Id.

n124. Id.

n125. See infra note 186 and accompanying text (presenting the main reason why law enforcement agencies have difficulty recruiting individuals with the specialized technological backgrounds).

n126. See, e.g., Margret Johnston, International Panel Testifies on Cyber Attacks, SunWorld, Aug. 2000, available at LEXIS, News Library, SUNWLD File (explaining how "an international panel of computer security officials told a U.S. congressional committee that a quicker response to cyber attacks is needed both between countries and between government and private industries").

n127. See id. (providing a statement by Ohad Genis, an Israeli police representative who is also the advocate and chief inspector of the National Unit for Fraud Investigations). While participating in the international panel of computer security officials, Genis voiced his concern that the response from other countries in computer crime investigations is too slow. Id. As an example, Genis cited a situation that took place during a recent round of Middle East peace negotiations at Camp David. Id.

The Israeli police continuously received information that there were Internet sites calling for the assassination of Israel's Prime Minister Ehud Barak. The Israeli authorities had to go through long procedures to try to identify the people responsible for the Net threats. In order to obtain the names of the users who use specific IP (Internet Protocol) addresses we still have to wait weeks and months.

Id.

n128. See, e.g., id. (describing the position of Juergen Maurer, the detective chief superintendent of the German Federal Police, who also

participated on the international panel of computer security officials that reported to a U.S. Congressional committee). "German authorities dealt with the U.S. National Infrastructure Protection Center (NIPC) in only one case ... that occurred in February. That case showed that, even though the cooperation was very good, there is still a need to establish a more efficient and effective way of exchanging information." Id. Maurer stressed the importance of forging cooperative partnerships with the system administrators of the affected companies that fall prey to cyber crimes as a way to obtain required information. Id. "Access to the desired data should be possible without having to go through the time-consuming formalities underlying international law... ." Id.

n129. See WWW.Commercial Terrorism.Com, supra note 123, at 178 (explaining that the individual users in Sweden and the United States were a computer science student and a computer engineering student, respectively).

n130. See id. "The unusual collaborators pinpointed the origin of the offending virus to a single telephone line in New Jersey." Id.

n131. See Sinrod & Reilly, supra note 7, at 219 (citing *18 U.S.C. 1030*(a)(2), (5)(A) as the applicable federal statute under which Smith pled guilty).

n132. See supra notes 101-13 and accompanying text (describing instances where virus authors escaped punishment because the jurisdictions in which they were found did not have adequate laws).

n133. See Soma, supra note 12, at 318 (espousing that "the process of extradition can be defined simply as the surrendering of a criminal or accused criminal by one sovereign to another").

n134. Id. at 317-18.

n135. See id. (examining the inability of extradition law to promptly respond to changes in criminal law, particularly with respect to computer crime).

n136. See id. at 322 (describing how "the United States, following international custom, requires formal extradition treaties").

n137. See id. (noting that the United States is party to over 100 extradition treaties with various nations around the world).

n138. See id. (defining reciprocity as "the notion that one sovereign will surrender fugitives so long as its own requests for fugitives will be honored"); see also id. at 318 n.2 (citing M. Cherif Bassiouni, International Extradition and World Public Order 1 (1974) as warning that reciprocity should not be confused with double criminality). "While double criminality creates mutual obligations, it should not be confused with reciprocity. Where reciprocity creates an expectation that the requesting state shall equally honor similar future requests, the doctrine of double criminality contemplates similar crimes." Id. at 324 n.34.

n139. See id. at 323 n.26 (explaining that not all countries follow U.S. policy of requiring formal treaties for extradition). "For example, France and Switzerland statutorily provide for extradition where no treaty exists. Common law countries, however, are more likely to require more formalistic treaty obligations." Id.; see generally *Factor v. Laubenheimer, 290 U.S. 276 (1933)* (interpreting international law as withholding a legal right to demand extradition unless a treaty is in place); see also *Valentine v. U.S. ex rel. Neidecker, 299 U.S. 5, 9 (1936)* (stating that the U.S. Constitution prohibits extradition unless provided for by law or treaty).

n140. See Soma, supra note 12, at 323 n.31 (explaining that double criminality is alternately referred to as "dual criminality" by some scholars). Other basic characteristics of a typical U.S. extradition treaty include the political offense exception, speciality, and procedural requirements. Id. at 322.

n141. See generally, id. at 322-23 (describing the concept of reciprocity).

n142. Id.

n143. See id. at 323 (describing the instances when reciprocity plays the largest role in extradition proceedings).

n144. Id.

n145. Id.

n146. See id. (noting that every treaty to which the United States is a party includes some form of double criminality language).

n147. See id. at 324 (explaining that "double criminality protects states' rights by promoting reciprocity and also safeguards individual rights by shielding the individual from unexpected and unwarranted arrest and imprisonment").

n148. When a treaty requires that both countries consider the act criminal in order to extradite, a computer criminal will not be subjected to extradition if one of the involved countries cannot prosecute the computer crime. Id.

n149. See Soma, supra note 12, at 346.

n150. See Bassiouni, supra note 12, at 330 (noting that "treaties do not define these offenses but only name them; and therefore, some body of substantive criminal law must be applied by the extradition magistrate to determine whether the act committed constitutes a treaty offense"); see also Soma, supra note 12, at 323-26 (describing the list of specific offenses within an extradition treaty as the "enumerative approach").

n151. See generally, Bassiouni, supra note 12, at 316-19 (explaining the "eliminative method" in detail).

n152. See Soma, supra note 12, at 325 (specifying that "the required minimum sentence length refers to the "potential' and not the "actual' sentence").

n153. See, e.g., supra notes 101-105 and accompanying text (describing how Taiwan had no computer crime legislation in place when the author spread the Chernobyl virus).

n154. See supra notes 73-78 and 105-10 and accompanying text (discussing the ILOVEYOU virus and its author's escape of prosecution).

n155. See Soma, supra note 12, at 351 n.212 (listing the prison sentences for some countries that criminalize the unauthorized access of computers with the intent to alter or damage data, regardless of whether such damage results). "Generally, the maximum imprisonment penalties are [as follows]: Australia-10 years; Canada-10 years; Finland-1 year; Germany-2 years; Japan-5 years; Netherlands-4 years; Sweden-2 years; U.K.-6 months; United States-5 years." Id.

n156. See, e.g., Soma, supra note 12, at 351 (describing how both U.S. and Australian law applied in United States v. Morris). However, if the worm had affected a computer other than one belonging to the government, a crime would only have been committed in the United States because Australian law only protects government computers. Id.

n157. See generally World's Richest Countries Call for Web Security Standards, Agence France Presse, Oct. 26, 2000, available at LEIXS, News Library, AFPFR File (stating that "Internet experts from the world's wealthiest countries attending a conference on cyberspace crime ... recommended international security standards to protect users"); see also Keith Nuthall, Confounding Cyber-Crime, Computer Wkly., Apr. 15, 1999, at 30, available at LEXIS, News Library, ASAPIN File (proposing that "the fight against computer crime requires an international response. Offences are often carried out from a remote site and possibly in a different country to the victim"); see also "Love Bug' Sparks Demand, supra note 73 (relaying the U.S. government's request that "a world summit be held to get countries to cooperate in protecting vital installations and companies from virulent virus attacks"); see also EDS Chairman and CEO Dick Brown Promotes Cyber Security at Global Business Dialogue; Brown Says Secure Internet is Key to Future of Digital Economy, PR Newswire, Sept. 26, 2000 (setting forth the Global Business Dialogue on Electronic Commerce's observations and policy recommendations to all governments "to promote a cooperative and international industry-to-government and government-to-government effort to enhance cyber security and to fight cyber crime").

n158. See, e.g., Soma, supra note 12, at 360-62 (explaining how amendments to U.S. legislation might be a way to facilitate extradition).

n159. Id. at 360.

n160. See id. at 361.

n161. See, e.g., id. (describing the Commonwealth Scheme and the U.K. Computer Misuse Act).

The Commonwealth Scheme provides for extradition between the members of the British Commonwealth without specific treaties. This scheme links over thirty States, including Great Britain, Australia, New Zealand, Canada, India, and the West Indies. The U.K. Computer Misuse Act, followed by some of the countries in the Commonwealth Scheme, already includes extradition language. Accordingly, the extradition of criminals in other Commonwealth countries is already possible among the participants. Id.

For a detailed discussion of the Commonwealth Scheme, see Shearer, supra note 12, at 54-57.

n162. Id. If the United States were to adopt the language of the Commonwealth Scheme described above, it could then engage in reciprocal extradition with nations that are signatories to the Scheme.

n163. See Soma, supra note 12, at 361.

n164. See id. (discussing why extradition language in legislation is of no use in areas such as Internet adult pornography, dangerous speech, and national security).

The inclusion of extradition language would not be helpful in those areas lacking international agreement on criminality ... because extradition cannot occur if the requested country and the requesting country disagree as to whether a behavior should be criminalized. For example, although added extradition language to the federal obscenity statute would establish double criminality in countries possessing equivalent legislation, it would not expand the number of countries willing to extradite for this offense. Similarly, in the category of dangerous speech, extradition would not be perfected to countries wishing to prosecute for speech offenses because the United States does not criminalize most speech ... . In some areas, such as national security, the inclusion of extradition language is wholly improper. National security is a national matter. Accordingly, seeking the inclusion of extradition language in such legislation could offend principles of sovereignty.

Id. at 362.

n165. See id.

n166. For further discussion surrounding other computer crimes in the context of extradition, see generally, Soma, supra note 12.

n167. Alan Boyle, MSNBC, Debating the World's Digital Gap (Oct. 18, 2000), at http://www.msnbc. com/news/478319.asp?cp1=1 (copy

on file with The Transnational Lawyer).

n168. See id. (reporting a speech made by Bill Gates, Microsoft Chairman, on "Creating Digital Dividends" in Seattle, Washington in October 2000).

Gates noted that [his self-established charitable] foundation's giving pattern was weighted about 60 percent toward health-oriented projects and 30 percent toward educational and library-related projects-and he said public health had to take priority in aid programs for the developing world. He cited figures indicating that millions of children die every year from age-old diseases that could have been prevented by existing vaccines. "I am suggesting that if somebody is interested in equity, you wouldn't want to spend more than 20 percent of your time talking about computers," he said.

Id.

n169. See supra notes 150-52 and accompanying text (contrasting the eliminative and numerative methods of drafting treaties).

n170. See Soma, supra note 12, at 323 (describing how the United States is a party to over 100 extradition treaties around the world).

n171. Id. at 369.

n172. See infra notes 182-83 and accompanying text (postulating the shortcomings of law enforcement working to combat cyber crime without the aid of the private sector and vice versa).

n173. See, e.g., infra notes 178-81 and accompanying text (outlining the cooperative efforts on Interpol and AtomicTangerine to combat cyber crime).

n174. See, e.g., infra notes 175-76 (describing two instances of outcry for a cooperative effort between law enforcement and the private sector).

n175. See Steve Ulfelder, Don't Tread on IT, Computerworld, Aug. 28, 2000, at 40, available at LEXIS, News Library, COMPTG File (recalling Former U.S. Attorney General Janet Reno's opinion that the federal government lacks the sophistication and technical resources that IT corporations possess, and that only cooperation between corporate entities and the government can ensure the United States' ability to prosecute cyber criminals). Janet Reno issued this opinion in June, 2000, according to a Computerworld report on June 19, 2000. Id.

n176. See id.; see also Nuthall, supra note 157, at 30 (discussing how the U.K. is also addressing the lack of IT expertise within a police force).

A liaison unit has been set up between the Association of Chief Police Officers and a group of Internet service providers, which has now broadened its remit, and staged seminars open to all computer professionals across the UK. The Serious Fraud Office employs 170 investigators to crack complex cases-many of which involve the use of computers, while the Metropolitan Police runs a 10-strong Computer Crime Unit.

Id.

n177. See id.

n178. Interpol and AtomicTangerine Announce Unique Alliance to Arrest the Multi-Billion Dollar Online Crime Wave, PR Newswire, June 30, 2000.

n179. Id.

n180. Id. (describing the innovative alliance between Interpol and Menlo Park-based venture consulting firm, AtomicTangerine, that will give companies worldwide "new access to superior intelligence in their war against global cyber crime"). The journey that led to this unprecedented alliance began in May 2000 at the Internet Defense Summit in the Silicon Valley, where top executives from American and European industry heard the Interpol Secretary-General warn that the private sector must defend itself because government agencies do not have the technology to do the job, and pledge Interpol cooperation for the fight. Id.

"Private sector companies have a responsibility to their stakeholders and to the public at large to protect their Internet activities,' said Interpol Secretary-General Rayond Kendall and AtomicTangerine CEO Jonathan Fornaci in a joint statement. "Assistance by Interpol can contribute to the private sector's essential self-defense. At the same time, information gathered by some private companies may be of substantial

assistance to government agencies.' AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide.

Id.

n181. See id.

n182. See infra note 248 and accompanying text.

n183. See id.

n184. See, e.g., Harrison, supra note 67 (describing how Germany believes that a specialized international organization should be established to deal solely with international cyber crises).

n185. See Ann Harrison, Warnings About Security Holes Abound at Def Con, SunWorld, Aug. 2000, available at LEXIS, News Library, SUNWLD File (describing the address Arthur Money, CIO at the Pentagon, gave during the opening session at the Def Con hackers convention). Money jokingly thanked audience members for withholding attacks against the Pentagon's systems during the Y2K transition and appealed to attendees to use their talents on behalf of the U.S. government. Id. Def Con, now in its eighth year, meets in Framingham each year and has grown from "a small private party to a large hacker social event featuring workshops on exploitable vulnerabilities, defense strategies and the latest in technology tools for the security community. It attracts hackers from around the world whose refined skills bedevil administrators everywhere." Id. Officials from the U.S. Central Investigation Agency, the National Security Agency, and the U.S. Department of Defense also attended the yearly convention in June 2000. Id.

n186. See generally Nuthall, supra note 157, at 30 (discussing the dilemma that companies and law enforcement agencies are not adequately equipped to detect and apprehend criminals "operating on the cutting edge of technical and business developments"). Cyber crime is growing and with it is the demand for police officers who understand computers. Id. The clear solution is to recruit from the corporate sector so that the police force can increase its arsenal of IT professionals. Id.

David Toddington, who runs his own company, warns that in Canada police resources are so stretched that private sector victims of computer crime are sometimes told that their grievances cannot be investigated. "If there is one message that you should be aware of,' Toddington says, "it is that you are on your own... ." Toddington explains that Canada is short of 20,000 IT professionals, while the figure is

closer to 200,000 in the U.S.

Id.

The main problem with the police forces' ability to recruit computer experts is that IT professionals earn higher salaries working in the private sector and would rather not take a pay cut to work for the government. Id. "In the private sector, IT professionals can command $ 140,000, while police salaries are usually closer to $ 60,000. Inevitably there is a real pressure on trained officers to pursue more lucrative options." Id.

n187. See generally John Revill, CyberCops to Lead War Against Internet Crime, Birmingham Post, Nov. 14, 2000, at 6, available at LEXIS, News Library, BIRPST File.

n188. See id. (reporting an announcement made by Home Secretary Jack Straw on Nov. 13, 2000).

n189. See generally Rebecca Paveley, Elite Cyber Cops Will Tackle Internet Crime-80 Strong Squad to be Set Up, The Journal (Newcastle, UK), Nov. 14, 2000, at 14, available at LEXIS, News Library, THEJRN File. "Each regional force will have at least one cyber cop to tackle Internet crime in their area." Id.

n190. See Revill, supra note 187, at 6.

n191. See generally New Hi-Tech Crime Investigators In #25Million Boost to Combat Cybercrime, Hermes, Nov. 13, 2000.

n192. Id.

n193. See Revill, supra note 187, at 6.

n194. This Comment reflects the current economic trends.

n195. See Nuthall, supra note 157, at 30 (exposing IT security consultant David Toddington's concerns surrounding Canada's shortage of IT professionals in comparison to the number in the United States). "In the private sector, IT professionals can command $ 140,000, while police salaries are usually closer to $ 60,000. Inevitably there is real pressure on trained officers to pursue more lucrative options." Id.; see also Interpol Calls For Corporate Help, Network News, May 17, 2000, at 2, available at LEXIS, News Library, NETNEW File (quoting Interpol Secretary General Raymond Kendall at the Internet Defense Summit as remarking that "we cannot afford to engage the technology, technicians and research resources necessary to find quick solutions to a relatively new phenomenon").

n196. See id. (pointing out that a minority of IT leaders applaud such global efforts because they recognize that one of the main issues facing IT is the inability to prosecute hackers). Alvin Boynton, manager of IT at Intranets.com Inc. in Woburn, Massachusetts, and others who attended the June Computerworld Premier 100 Conference for IT Leaders point to the Love Bug as an example of how cyber criminals will get away if international laws and agreements are not promulgated. Id.

n197. Ulfelder, supra note 175, at 40 (providing that 89% of IT leaders at the June 2000 Computerworld Premier 100 Conference for IT Leaders believed security was the number one issue, but still preferred a limited role (62%) or no role at all (14%) in U.S. federal government security). Only 21% preferred that the government play a substantial role. Id. Seventy-one attendees completed a survey on government and IT). Id. Linda Rossetti, CEO of Boston-based eMaven, Inc. added: "We're delighted for the [feds] interest, ... but how solvable is the issue politically? The data security problem is less about control than it is about education." Id. Linda Rossetti further asserted that education on security practices and tools is best left to organizations and IT departments. Id.

n198. Paul K. Ohm, On Regulating the Internet: Usenet, A Case Study, Comment, *46 UCLA L. Rev. 1941, 1959 (1999).*

n199. See supra notes 196-206 and accompanying text, see also infra notes 237-59 and accompanying text (discussing why many private sector and civil rights groups are opposed to government regulation of cyber crimes).

n200. See Ohm, supra note 198, at 1959-60.

n201. See id. (expressing concern with legislators' abilities to comprehend the intricacies of computer crimes). "Internet technology ... descriptions are often rife with complex acronyms and arcane networking concepts. Lawmakers who do not understand the Internet space they are regulating tend to write laws that either fail to solve the problem or injure the regulated space." Id.

n202. See id.

n203. See generally Robin A. Brooks, Deterring the Spread of Viruses Online: Can Tort Law Tighten the "Net'?, *17 Rev. Litig. 343 (1998)* (discussing the ability of tort liability to handle and adequately spread the costs of damage caused by computer crime to ISPs and software distributors).

n204. See *id. at 345.*

n205. *Id. at 346.*

n206. See *id. at 346 n.8.*

n207. See Dressler, supra note 14, at 27-77 (providing a complete discussion about theories on deterring punishment).

n208. The U.S. statute that criminalizes computer crimes such as the spread of viruses allows for the victim to bring a civil tort action against the author if the damage caused is over $ 5,000. See *18 U.S.C. 1030*(g) (2000). This is in addition to the criminal charges and serves as an incentive for private sector corporations to report these security breaches to the authorities. See Nicholson, supra note 49, at 216.

n209. See id. (discussing a remedy in tort for victims of computer crimes under *18 U.S.C. 1030*(g)).

n210. Paul Meller, Council of Europe to Discuss Cyber Crime Treaty, InfoWorld Daily News, Nov. 22, 2000, available at LEXIS, News Library, INFDLY File.

n211. See id. (mentioning that some members of the Council of Europe "automatically adopt Council treaties once they are passed" while "others would be obliged to pass their own legislation to conform with the treaty"); see also Cybercrime Treaty Raises Regulatory, Privacy Concerns, Info. Security, June 2000, at 19, available at LEXIS, News Library, INFSEC File [hereinafter Treaty Raises Concerns] (stating that "the Council of Europe consists of more than 40 signatory nations, including non-European countries such as the United States, Canada, Japan, Russia and South Africa").

n212. See Robert Lemos, MSNBC, Coalition Slams Cybercrime Treaty (Oct. 19, 2000), at http://www.msnbc. com/news/478718.asp (copy on file with The Transnational Lawyer) (explaining that "while the United States is not a part of the 41-member Council of Europe, members from the U.S. Department of Justice and the FBI have aided in the drafting of the treaty").

n213. Dorothy E. Denning, Disarming the Black Hats?, Info. Security, Oct. 2000, at 16, available at LEXIS, News Library, INFSEC File.

n214. See Treaty Raises Concerns, supra note 208, at 19 (adding that other provisions of the Draft Convention on CyberCrime not relevant to this Comment address child pornography, computer-related forgery and fraud).

n215. See Denning, supra note 213, at 16.

n216. The Council of Europe, Draft Treaties, available at http://www.coe.int (copy on file with The Transnational Lawyer).

n217. See Patrick Thibodeau, European Cyber Treaty Raising Concerns, Computerworld, Dec. 11, 2000, at 12, available at LEXIS, News Library, COMPTG File.

n218. Lemos, supra note 212.

n219. See Draft Convention on Cyber-Crime, Draft No. 25 Rev., Dec. 22, 2000, ch. 2, sec. 1, tit. 1, art. 2, at http://www.coe.int (copy on file with The Transnational Lawyer) [hereinafter Draft Treaty] (stating that "each party shall adopt such ... measures ... to establish as criminal offences under its domestic law when committed intentionally the access to the whole or any part of a computer system without right ...").

n220. See id. at ch. 2, sec. 1, tit. 1, art. 4, 5 (stating that "each party shall adopt such ... measures ... to establish as criminal offences under its domestic law when committed intentionally ... the damaging, deletion, deterioration, alteration, or suppression of computer data without right," and "the serious hindering without right of the functioning computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data").

n221. See id. at ch. 2, sec. 1, tit. 1, art. 6.

Each Party shall adopt such ... measures ... to establish as criminal offences under its domestic law when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5;

2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2-5... .

Id.

n222. See id. at ch. 2, sec. 1, tit. 5, art. 12.

Each Party shall adopt ... measures ... to ensure that a legal person can be held liable for a criminal offence ... committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person... .

Id.

n223. See id. at ch. 2, sec. 2, tit. 2, art. 16.

1. Each Party shall adopt such ... measures ... to enable its competent authorities to order or similarly obtain the expeditious preservation of [specified] computer data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to Paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt ... measures ... to oblige that person to preserve and maintain the integrity of that computer data for an adequate period of time, as necessary, to enable the competent authorities to seek its disclosure... .

Id.

n224. See id. at ch. 3, sec. 1, tit. 1, art. 24.

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or the proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Id.

n225. See id. at ch. 3, sec. 1, tit. 2, art. 25. "This article applies to extradition between Parties for the criminal offenses established in ... this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty... ." Id.

n226. See Harrison, supra note 67.

n227. Id.

n228. See Denning, supra note 213, at 16 (comparing the possession and sale of "cyberweapons" to the possession and sale of firearms).

In many countries, the use of cyber-weapons is now a crime, but the development, distribution and acquisition of these tools remain legal

(with the exception of tools that circumvent copyright protection and clone cellular phones). By comparison, the possession, sale and transportation of firearms is highly regulated by domestic laws and international treaties.

Id.

n229. Id.

n230. See generally supra notes 157-209 and accompanying text (outlining other solutions proposed to combat the problem of **prosecuting computer virus authors** internationally).

n231. See supra notes 158-63 and accompanying text.

n232. See supra notes 169-70 and accompanying text.

n233. See generally Draft Treaty, supra note 219.

n234. See generally Draft Treaty, supra note 219.

n235. Id.

n236. See id.

n237. See infra notes 241-47 and accompanying text.

n238. See infra notes 243-47 and accompanying text.

n239. See infra notes 248-51 and accompanying text.

n240. See infra notes 252-59 and accompanying text.

n241. Bob Sullivan, MSNBC, Cybercrime Treaty Targets Hackers (Oct. 24, 2000), at http://www/msnbc. com/news/480734.asp (copy on file with The Transnational Lawyer).

n242. See, e.g., supra note 238 (discussing that the possibility of a restrictive treaty of this kind scares many top European computer security experts).

n243. See Sullivan, supra note 241.

n244. See id. (noting that the Draft Treaty includes aiding-and-abetting rules that appear to make the publishing of software vulnerabilities or exploits illegal). According to U.S.-based cyberlaw expert Jennifer Granick, the Treaty could make vulnerability mailing lists illegal. Id.

n245. See, e.g., Bob Sullivan, MSNBC, High-Stakes Hacking, Euro-Style (Oct. 23, 2000), at http://www.msnbc.com/news/479105.asp (copy on file with The Transnational Lawyer) (noting that in Europe, many computer security experts called "white hat" hackers find vulnerabilities and make their work public). A "white hat" publishes the security flaws he discovers on his NTBugTraq mailing list. Id.; see also Sullivan, supra note 54 (explaining that vulnerability mailing lists, such as BugTraq and NTBugTraq, which are used in good faith to promote security on the Internet are illegal under the Draft Treaty). Both BugTraq and NTBugTraq have well over 30,000 subscribers. Id.

n246. See id. (quoting Granick's comment, "hacking software poses special challenges because most of the tools have two equal uses").

For example, a popular hacking tool called nMap connects to a remote computer and tells the user if that computer has any open ports than can be used to establish a connection. Finding such a port is often the first step in a computer attack, making nMap popular among attackers. But the program is equally popular with network administrators who want to check their own systems for open ports.

Id.; see also Ted Bridis & Rebecca Buckman, MSNBC, Microsoft's Network is Hacked (Oct. 27, 2000), at http://www.msnbc.com/news/481927.asp?cp1=1 (copy on file with The Transnational Lawyer) (illustrating an additional example of using legal software in an illegal way). On Wednesday, Oct. 25, 2000, Microsoft security employees discovered a computer break-in. Id. Microsoft believes the hackers stole blueprints to its most valuable software. Id. Those familiar with the case speculate that the hackers initially gained access to Microsoft's corporate computers by using hacker software called the QAZ Trojan. Id.

n247. See Denning, supra note 213, at 16.

n248. Id.; see also Lesley Stones, Forty Nations Unite to Define Cybercrime and Fight Net, Bus. Day (South Africa), Nov. 2, 2000, at 20 (reporting that "many service providers believe that such clauses would breach the confidentiality agreements they sign with their customers").

n249. See, e.g., Harrison, supra note 67 (explaining that Senator Fred Thompson, R-Tenn., warned that Congress should not pass legislation that forces companies to cooperate with investigations).

n250. Id.

n251. See Ann Harrison, Strategies for Fighting Computer Crime Shared at Security Summit, InfoWorld Daily News, May 10, 2000, available at LEXIS, News Library, INFDLY File (noting that Senator Fred Thompson, R-Tenn, drafted and announced a bill calling for annual reviews of government security practices).

"We don't know yet how to run our own shop,' Thompson acknowledged, adding that companies have to create their own security defense plans. He said that government could assist by providing grants for security research, granting tax breaks to companies that develop security tools, enforcing current laws, and increasing the number of visas for high-tech workers.

Id.

n252. See id. (noting that David Banisar, staff counsel for the Electronic Privacy Information Center, in a protest letter, voiced his prediction that the civil sector would not like the implications of the Draft Treaty either). "I imagine that the industry guys are not going to be too thrilled either." Id.

n253. See infra notes 256-59 and accompanying text.

n254. See generally Statement of Principles, Global Internet Liberty Campaign, at http://www.gilc.org/ about/principles.html (visited Nov. 8, 2000) (copy on file with The Transnational Lawyer) (explaining the policies that the GILC advocates). Some of the GILC policies include "insisting that on-line free expression not be restricted by indirect means such as excessively restrictive governmental or private controls over computer hardware or software, telecommunications infrastructure, or other essential components," and "allowing on line users to encrypt their communications and information without restriction." Id.; see also Member Organizations, Global Internet Liberty Campaign, at http://www.gilc.org/about/members.html (visited Nov. 8, 2000) (copy on file with The Transnational Lawyer) (listing the member organizations of the GILC).

n255. See Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, Global Internet Libery Campaign, Oct. 18, 2000, at http://www.gil.org/privacy/coe-letter-1000.html (copy on file with The Transnational Lawyer) [hereinafter GILC Protest Letter] (re-printing the protest letter from GILC to the Council of Europe Secretary General Walter Schwimmer). The GILC includes groups from the United States, France, Britain, Australia, Bulgaria, Canada, Italy, South Africa, Austria, the Netherlands, and Denmark. Id.

n256. See Lemos, supra note 212 (claiming that the treaty "is little more than a law enforcement wish list").

n257. Id.

n258. Id.

n259. See GILC Protest Letter, supra note 255. The GILC protest letter stated that "police agencies and powerful private interests acting outside of the democratic means of accountability have sought to use a closed process to establish rules that will have the effect of binding

legislation"); see also Lemos, supra note 212.

"It is in some sense an endrun' said Jim X. Dempsey, senior staff counsel for the Center for Democracy and Technology, a policy think-tank. "The concern here is that the U.S. government is going overseas to promote in whatever international forum it can find, an expansion of authority that is has not been able to acquire here.'

Id.

n260. See Nicholson, supra note 49, at 254 (listing these necessary elements).

n261. See supra note 155 and accompanying text (listing the lengths of sentences for computer crimes in various nations).

n262. See Boyle, supra note 167.

N263. Id.

n264. See Draft Treaty, supra note 219 (citing to draft number 25 that was declassified by the Council of Europe on Dec. 22, 2000, and is the most current draft of the Treaty as of the date of publication of this Comment).

n265. Denning, supra note 213, at 16 (conveying the concern of Purdue University's Gene Spafford that "some countries might construe the mere possession of ... software [intended for security research] as intent of malicious activity").

n266. Id.