Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law

By Susan W Brenner
University of Dayton School of Law

Contents

Introduction

1. The development of the Internet and the proliferation of computer technology has created new opportunities for those who would engage in illegal activity.[1] The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appear to be some new varieties of criminal activity.[2] Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement. [3]

2. This article argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. These legal tools include an arsenal of well-defined cybercrime offenses for use in prosecuting cybercriminals and procedural rules governing evidence-gathering and investigation. [4] Because cybercrime is often transnational in character, offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. [5] It is, therefore, important that every legal system take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes.

3. Section II of the article provides an overview of the problems cybercrimes pose for law enforcement officials. Section III reviews the kinds of offenses that qualify as cybercrimes and points out how existing law can be deficient in this regard, e.g., where penal law often fails to encompass the kinds of activities cybercriminals engage in. Section III also discusses the extent to which new laws are needed to address these activities and considers whether existing laws can be modified so that they are adequate for this purpose. Section IV briefly reviews some of the obstacles procedural law can present for the investigation and apprehension of cybercriminals. While the focus of the article is primarily on penal law, inadequacies in penal and procedural law can interact to allow cybercriminals to evade responsibility for their actions. Section IV therefore examines jurisdictional limitations and the difficulties that arise when the procedural laws of different countries place inconsistent and conflicting limitations on the evidence-gathering process.

4. The primary focus of the article is on penal laws simply because there tends to be more consistency in the way countries define criminal offenses than there is in the area of procedural law. Much of this is due to simple empirical necessity: In order to maintain the level of internal stability a nation must enjoy to survive and prosper, each country must have penal laws that protect the safety of individuals ("crimes against persons"), that preserve the integrity of at least certain types of property ("crimes against property"), that prohibit interference with the legal system ("crimes against the administration of justice"), and that proscribe attacks on the government ("crimes against the state"). While each nation will vary in how it defines the discrete offenses that fall into these categories, one can assume a certain generic consistency in penal laws. That generic consistency makes it possible to discuss general strategies nations can employ in adapting their penal laws to deal with the problem of cybercrime. It is, however, not possible to postulate the same level of generic consistency with regard to procedural law; although there are empirical constancies in the procedures law enforcement uses when investigating and prosecuting crimes, nations vary widely in the legal constraints they place on these processes. For that reason, the discussion will note areas of procedural law that are important in dealing with cybercrimes, but this portion of the discussion will be more general than that in Section III, which deals with the penal law.

Cybercrime: An Overview of the Problem

5. In early May of 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe. According to one report, the virus, which was designed to disseminate itself and to destroy various kinds of files on a victim's computer, "infected at least 270,000 computers in the first hours" after it was released.[6] The "love bug" forced the shutdown of computers at large corporations such as Ford Motor Company and Dow Chemical Company, as well as the computer system at the House of Lords.[7]

6. After security experts determined that the virus had come from the Philippines, investigators from the Philippines and from the United States set about

tracking down the person(s) who created and disseminated it. They were frustrated in this effort by the Philippines' lack of computer crime laws: For one thing, it took days for investigators to obtain a warrant to search the home of their primary suspect; local prosecutors had to comb through Philippines statutes to find laws that might apply to the dissemination of the virus, and then had to persuade a judge to issue a search warrant on the basis of one possibility.[8] For another, when a suspect-Onel de Guzman-was eventually apprehended, there were no laws criminalizing what he had done. The Philippines had no statutes making it a crime to break into a computer system, to disseminate a virus or other harmful software or to use a computer in an attempt to commit theft. Lacking the ability to charge de Guzman with precisely what he had done-e.g., with disseminating a virus-Philippine prosecutors charged him with theft and with violating a statute that covered credit card fraud.[9] Those charges were eventually dropped after the Department of Justice determined that "the credit card law [did] not apply to computer hacking and that investigators did not present adequate evidence to support the theft charge." [10]

7. The "love bug" destroyed files and impeded e-mail traffic in more than twenty countries. [11] Some estimated that the virus caused $10 billion in damage, much of that in lost productivity.[12] The episode prompted the Philippines to adopt a cybercrime law that established fines and prison sentences for those hacked into computer systems and/or disseminated viruses or other harmful programs.[13] The new law could not be applied retroactively against the individual suspect of disseminating the "love bug" virus, so that crime went uncharged.[14]

8. The "love bug" episode is instructive for those who are concerned about cybercrimes because it so clearly illustrates some of the problems this type of activity poses for law enforcement, i.e.:

    1. The lack of cybercrime-specific penal laws and/or the inadequacy of penal laws that were crafted to deal with criminal conduct occurring in the real, physical world, not in or by means of the virtual world of cyberspace;

    2. The lack of international agreements on cybercrimes which exacerbates the problems posed by the lack/inadequacy of local penal law and the oftenconflicting requirements local procedural laws;

    3. The difficulty of ascertaining which nation(s) has/have jurisdiction to prosecute a cybercriminal and, once this determination has been made, of asserting jurisdiction over that person;

    4. The difficulty of determining how many offenses have been committed, against whom and the damage resulting from those offenses.[15]

9. Because of these and other issues, cybercrimes are a challenge for every nation, a challenge countries must address both individually and collectively.

10. Individually, each nation must examine its own penal and procedural law to determine whether they are adequate for dealing with the so-far-identified varieties of cybercrimes. The "love bug" forced the Philippines to do this, at least insofar as its penal laws were concerned, and to adopt at least some remedial legislation. The Philippines government was forced to act, in large part, by the international outcry that arose as a result of the damage the "love bug" caused in other countries;[16] the virus seems to have had little effect within the Philippines. [17] But that is not always true; cybercriminals prey on their own countrymen as well as on people from other nations. Countries must, therefore, review their penal laws to ensure that they are adequate to protect their own citizens from cybercriminals, as it is not uncommon for internal prosecutions to fail for lack of applicable law.[18] If a country's review reveals that its penal laws are not adequate to deal with the so-far-identified varieties of cybercrime, it should immediately take steps to remedy the deficiencies, either by adopting new cybercrime-specific laws or by amending its existing laws so that they encompass cybercrimes.

11. Because technology has made national borders permeable, cybercrime is not a phenomenon that can be dealt with only at the national level; as the "love bug" episode illustrates, with the emergence of cybercrimes we witness the correlate development of "remote offenders," perpetrators who can, while physically located in one country, easily wreak havoc in other nations. [19] International cooperation is required to deal with the cybercrime as a transnational phenomenon, e.g., with the offender who, working from a computer in County A, embezzles funds from a bank in County B or steals trade secrets from a corporation in County C.[20] If Country A does not have penal laws in place that outlaw the offender's conduct, we have a "love bug" scenario, e.g., the offender will not be prosecuted in his own country (indeed, he may even be regarded with admiration in his own country), [21] and Country A will not extradite him so he can be prosecuted in Country B and/or Country C.[22] Alternatively, if Country A has penal laws prohibiting the conduct at issue, it may allow the offender to be extradited to Country B or Country C, but its procedural laws may not allow/require it to give those countries access to critical evidence that is located in Country A, evidence without which prosecution may be a de facto impossibility.[23] Cybercrime cannot, therefore, be treated as a "local" phenomenon; when it comes to dealing with cybercrime, no country is an island.[24] Instead, nations must cooperate to deal with the problem of cybercrime by ensuring that cybercriminals cannot exploit gaps and loopholes in procedural laws to evade capture and prosecution.

Penal Law: Old and New Offenses

12. The previous section explained why countries need penal laws that adequately address cybercrime. But according to one estimate, over 100 countries do not have penal law adequate to deal with cybercrime.[25] And last year a study examined the penal laws of fifty-two countries and found that thirty-three of them had not "yet updated their laws to address any type of cyber crime." [26]

13. What do assessments such as these actually establish? Both of these focused

on whether the countries in question had adopted new cybercrime-specific penal laws,[27] especially laws targeting "high-profile" cybercrimes like hacking, virus dissemination, fraud and theft, [28] and both were no doubt accurate in their respective evaluations of these matters. But the real question is whether the assumption implicitly underlying these assessments and others like them, i.e., that new cybercrime-specific penal laws are needed to deal with the problems posed by computer-generated crime because traditional penal laws are inadequate for this purpose, [29] is correct. That assumption, which is widespread, rests on the premise that "cybercrime" is a distinct, unitary phenomenon, a new class of anti-social activity that cannot be dealt with through the application of extant laws.

14. This premise and the assumption it gives rise to are in fact flawed, products of an oversimplification. As the remainder of this section demonstrates, "cybercrime" actually consists of a variety of discrete conduct, some of which can be reached under traditional penal law, some of which requires the modification of traditional penal law and some of which does, indeed, require the adoption of new penal laws. Rather than being a new phenomenon, "cybercrime" is simply the exploitation of a new technology to commit old crimes in new ways and, concededly, to engage in a limited variety of "new" types of criminal activity.[30]

15. It might seem logical to structure the discussion which follows around these categories, i.e., to examine crimes that can be prosecuted under existing laws, crimes that can be prosecuted if existing law is modified and crimes the prosecution of which requires the adoption of new, cybercrime-specific penal laws. That is not the best approach because such a categorization ignores the internal logic of any penal code's offense structure. The more appropriate way to proceed is by analyzing offenses according to the traditional, empiricallyderived categories into which they fall, e.g., "crimes against persons," "crimes against property," "crimes against morality," "crimes against the administration of justice" and "crimes against the state." [31] The sub-sections below analyze the need for cybercrime legislation-either new penal laws or the modification of existing penal laws-to address offenses falling into each of these broad categories. The discussion is not intended to be an exhaustive treatment of every offense falling into each category; it is, instead, an illustrative examination of the extent to which traditional offenses can be extrapolated to encompass computer-related criminal activity.

Crimes Against Persons

16. Crimes against persons can be divided into sexual crimes and non-sexual crimes.[32] Non-sexual crimes against persons include, inter alia, homicide (causing the death of another person),[33] assault (causing bodily injury to another person)[34] and threats. [35] Sexual crimes against persons include, inter alia, rape and child pornography.[36] The traditional offense-definitions used to deal with both categories of crimes developed in the context of activity occurring in the real, physical world, e.g., with physical assaults and with "real world" rapes.[37] And it might seem that there is no need even to include these offenses in a discussion of cybercrime law, on the assumption that they cannot

be committed in or via the "virtual world" of cyberspace but must involve actual physical confrontation between two or more persons.

17. That is, however, not the case. It would, for example, be possible to commit homicide by hacking into the computer system of a hospital and altering the records establishing the type and dosage of medication a patient is to receive so that the patient actually receives a lethal dose of medication.[38] This is a traditional offense-murder-being committed in a non-traditional fashion, by a perpetrator who may be hundreds or even thousands of miles away from the victim at the time death occurs. As such, it is certainly an example of the "remote perpetrator" scenario discussed in Section II of this article. The offender may be in another jurisdiction, and this may well present serious problems of identifying and apprehending the perpetrator. This scenario does not, however, give rise to difficulties with regard to the application of criminal liability for the act of causing the victim's death: It is reasonable to assume that every nation will have laws making it an offense to cause the death of another human being, simply because no modern state can survive if individuals are allowed to commit murder at will. As a matter of general principle, there is, therefore, little or no doubt that the perpetrator, once identified and located, can be extradited for prosecution to the jurisdiction where the victim died.[39]

18. In the homicide scenario described above, the computer is simply a tool used to commit a crime that is as old as mankind itself. Humans adapt technology to various uses, legitimate and illegitimate. Here, the computer substitutes for the knife, the gun, poison and any of a variety of other methods humans use to take the lives of their fellows. [40] And since legal systems do not generally parse homicide offenses according to the types of instrument used to inflict death, [41] e.g., "homicide by poison," "homicide by knife," "homicide by gun," etc., there appears to be no need to incorporate the use of the computer into extant homicide statutes. [42] This is a prime instance of a situation in which traditional penal law is adequate to address the use of a computer in the commission of criminal activity.

19. It is rather more difficult to hypothesize how a "remote perpetrator" could use a computer to commit an assault, inflicting bodily injury on another person. This could, perhaps, be done if the perpetrator were able to use to the computer to engineer some product defect or engineering calamity that he knew was sufficient to inflict bodily injury without causing death.[43] If this were done, the result is analogous to that set out above for computer-facilitated homicide, e.g., the legal system should be able to impose liability on the perpetrator by using its traditional penal law and prosecuting him for assault.

20. The same is true, and is not true, for non-corporeal attacks on another person: Penal laws have historically made it an offense to threaten another person with bodily injury or death.[44] The offense arose to deal with face-to-face threats (which arguably carry a greater threat of imminent danger), but the law had no difficulty accommodating threats transmitted by other means, such the postal service and/or telephone.[45] By the same token, extant law can be used to prosecute an offender if she uses a computer to transmit a threat to cause bodily injury or death.[46] Here, too, the computer simply becomes another

tool used to carry out a traditional offense. [47]

21. But that does not exhaust the analysis of non-corporeal attacks on another person: The rise of computer-generated and -transmitted communication has made it possible for perpetrators to engage in conduct that harasses and intimidates other persons without, however, rising to the level of "threatening" bodily injury. [48] This is illustrated by a case that arose in the United States of America, under federal law. Section 875 of title 18 of the U.S. Code makes it a federal crime, inter alia, to transmit a threat to injure another person in interstate or foreign commerce.[49] In United States v. Alkhabaz, [50] a federal court of appeals upheld the trial court's dismissal of charges that Jake Baker, also known as Alkhabaz, violated 18 U.S. Code ' 875 because it found that he did not transmit a Acredible threat@ to his alleged victim.[51] Baker, a student at the University of Michigan, had used e-mail to correspond with a friend; much of Baker's part of the correspondence consisted of vivid descriptions of fantasized sexual violence against a woman whose name was the same as that of one of his classmates.[52] When the correspondence came to light, he was prosecuted under 18 U.S. Code ' 875 for sending Athreats@ via interstate commerce.[53] The district court dismissed the charge because it found that the e-mail correspondence did not constitute Atrue threats@ and was therefore speech protected by the First Amendment to the U.S. Constitution.[54] The Sixth Circuit affirmed the dismissal because it agreed that the e-mail correspondence did not rise to the level of a Athreat.@[55]

22. The Alkhabaz case is one instance in which existing law proved to be inadequate to deal with computer-facilitated anti-social conduct. Other examples abound, some of which were ultimately addressed by the amendment of existing law or the adoption of new penal law.[56] Stalking, or cyberstalking, is an example of conduct which has so far tended to elude the reach of the criminal law; in the United States, for example, there is no federal anti-cyberstalking penal law, and few of the several U.S. states have enacted legislation which reaches cyberstalking. [57] In 1999, the U.S. Department of Justice issued a report which, among other things, articulated the dangers cyberstalking poses for its victims and the challenges it poses for law enforcement:

23. [C]yberstalking shares important characteristics with offline stalking. Many stalkers - online or off - are motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end. . . . Given the enormous amount of personal information vailable through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes.

24. . . . . [S]talkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and nonconfrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. . . . [W]hereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, . . . online

harassment . . . may be a prelude to more serious behavior, including physical violence.

25. . . . [T]he Internet and other communications technologies provide new avenues for stalkers to pursue their victims.

26. A cyberstalker may send repeated . . . messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal. California law enforcement authorities say they have encountered situations where a victim repeatedly receives the message "187" on their pagers - the section of the California Penal Code for murder. In addition, a cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyberstalker or others -- will have the intended effect on the victim, but the cyberstalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender. [58]

27. In one California case, the stalker-Gary Dellapenta--posed online as his female victim, who had spurned his romantic advances, and posted notices saying she wanted to be raped; when men responded to the notices, the stalker gave them her name, home phone number, address and advised them how to disable her home security system.[59] At least six different men showed up at the woman's home prepared to carry out what they thought was her request; she and her father were ultimately able to track the messages to Dellapenta, whom they reported to the police. [60] Fortunately, California did have penal law that could be used to prosecute such activity, [61] so when Dellapenta was identified he was charged, convicted and sentenced to serve six years in prison for what he had done.[62]

28. The Dellapenta case illustrates how computer technology can give rise to new types of antisocial activity: Dellapenta was able, in effect, to use others as his "weapons" against his victim, with the "weapons" being unaware they were endeavoring to engage in criminal activity. Dellapenta was also able to carry out his activities with anonymity, at least for a time; this only intensified the victim's terror, as she had no idea why the men were appearing at her home.[63] Scenarios such as these-which are not uncommon and are only likely to increase in incidence [64] -pose difficulties not only for law enforcement officers investigating such activity but also for the legal system's ability to impose criminal liability if and when the perpetrator is apprehended. Many jurisdictions do not have stalking laws, let alone cyberstalking laws, and those that do tend to require that the perpetrator actually communicate a "threat" of bodily injury to the victim. [65]

29. As the Dellapenta and Alkhabaz cases illustrate, computer technology and the rise of computer-facilitated communication require that jurisdictions carefully

assess what kinds of penal laws are needed to address phenomena such as cyberstalking and/or online harassment. [66] The cyberworld can give a perpetrator the ability to inflict psychic damage on a victim without ever actually threatening to inflict physical harm, as in the case of Gilbert Davis. Davis was an American student who, among other things, created a web site containing an image of his former girlfriend's "head transforming into a skull." [67] If Davis were to be prosecuted under the statute used in Alkhabaz or a similar provision, he would no doubt succeed in having the charges dismissed on the theory that his conduct did not rise to the level of communicating a "threat" because the web site's contents were not specifically directed to the "victim." Indeed, Davis could perhaps argue that his web site's contents were "art," an homage to the woman he claimed to still love. Can/should posting artificial constructs on the Internet give rise to the imposition of criminal liability?

30. Any attempt to answer this question has to include a consideration of sexual crimes against persons-e.g., rape and child pornography-as well as a consideration of activities such as cyberstalking and online harassment. [68] So far, there has only been one reported instance of "virtual rape" on the Internet, a case which arose when "virtual characters" participating in an online "virtual community"-LambdaMOO--were forced to engage in sexual activity against the will and inclinations of the individuals who had assumed those characters.[69] The case has given rise to debate as to whether "virtual crimes" can give rise to prosecution in the "real world." [70] Since activity such as the incident in LambdaMOO occurs only in cyberspace, it is not encompassed by the provisions of existing penal laws prohibiting rape and other physical attacks. [71] Indeed, much of penal law is predicated on the concept of some physical injury to person or property, which leads many to argue that criminal liability should not be imposed for "sexual assaults" occurring entirely in cyberspace. [72] Those who take this view argue that incidents such as the LambdaMOO attack are more properly handled within cyberspace, especially when the activity involved those who jointly chose to participate in an online activity such as the virtual community where this incident occurred. [73]

31. While that argument may be appealing when "virtual sexual assaults" occur among what are, in effect, consenting adults, its appeal weakens when the assault is directed at someone who may have had no contact with the perpetrator and who, at the very least, cannot be said to have consented to the attack. A law enforcement officer in the United States described this scenario to the author: Assume a man lives next door to a woman; the man videotapes the woman as she walks outside, perhaps going from her home to her automobile. Using computer technology, the man then "morphs" the woman's head and face onto the body of a woman in a pornographic video and posts the morphed video onto a web site. [74] The victim can now see herself being raped on the web site, as can members of her family, her employer, etc. Is this a crime? Should it be a crime? If it should be a crime, what is the crime-is it a form of rape? There is no physical assault. So should this be treated as an entirely new category of crime, one that encompasses cyberstalking and

harassment and other types of behaviors that are likely to crop up as computer technology becomes more sophisticated? Or should this not be a basis for imposing criminal liability-should the victim be limited to bringing a civil suit for damages and/or injunctive relief against the perpetrator? [75]

32. A variation of this issue will be decided by the United States Supreme Court some time next year: The Supreme Court has agreed to decide whether a federal criminal statute which targets child pornography can criminalize pornography produced by the use of "morphing" techniques-in which the images of adults are altered so they appear to be children.[76] The Ninth Circuit U.S. Court of Appeals struck down the portion of the statute that targets this "virtual child pornography," in part because it found that the statute violated the First Amendment in that there was no "compelling" government need to prohibit pornography the production of which did not involve the use of actual children. [77] Other U.S. Courts of Appeal have reached the opposite conclusion, [78] which is why the U.S. Supreme Court has agreed to decide the matter.

33. Regardless of what the U.S. Supreme Court decides in this case, the problem of determining whether, and when, criminal liability should be imposed for creating and disseminating artificial constructs and manipulating information that is freely available about individuals will persist.[79] This is an area that is not easily addressable, if at all, under existing penal legislation because, unlike computer-facilitated homicide, the conduct at issue does not consist simply of using computer technology as a means of committing offenses that have long been recognized by the penal law. [80] This is in essence "new" criminal activity--the conduct at issue exploits computer technology to achieve results that would not have been achievable in years past. [81] This is also an area that raises extraordinarily difficult legal questions for any nation that desires to maintain a balance between protecting the safety and security of individuals and guaranteeing the free dissemination of information and opinion. For all these reasons, this is an area that will present great challenges to those responsible for devising the penal laws of different nations; they will have to decide how this balance should be struck.

Crimes Against Property

34. There are many different types of crime against property, but because this is an illustrative, not an exhaustive, treatment of the interaction of computer technology and criminal activity, this section will focus on only a few: hacking, theft and forgery. Since, as is explained below, it is clear that computer technology is means of committing the traditional crimes of theft and forgery but this is not so clear with regard to hacking and related offenses, the discussion will begin with theft and forgery and conclude with an analysis of hacking and analogous activities.

35. As section II(A) explained, using a computer to cause the death of another human being (by changing prescription records, say) does not constitute the commission of a new offense, "cyberhomicide." It is simply employing a new implement to commit an old crime, just as those with murderous intent at

some point learned electricity could be used to cause death. The same is true for theft and forgery crimes, though perhaps it is more accurate to say the same can be true for these crimes, since the proliferation of computer technology and the concomitant increase in the number and types of intangible property concededly necessitates some revisions in the approaches to theft and forgery found in traditional penal laws. [82]

36. Theft crimes take different forms, [83] but the essence of theft is unlawfully taking property that belongs to someone else[84] The taking can be accomplished by appropriating and carrying away property (larceny), by using force to take property from another person's possession (robbery), [85] by deception (fraud), [86] by threats (extortion), [87] by breaking and entering (burglary) [88] or by exploiting a position of trust (embezzlement). [89] Theft in cyberspace is analogous to "real world" theft insofar as it recapitulates most, if not all, of these different forms of "taking" property, but it also differs in one important respect.

37. As to the analogies, computer-facilitated theft consists of using a computer to gain possession of ("take") property. The primary distinguishing factor of cybertheft is that it relies on the electronic transmission and manipulation of data-rather than acts and communications effected in the "real world"-- to effect a transfer of property from the rightful owner to the thief. In cyberextortion, the threats used to convince the victim to surrender her property are transmitted electronically; [90] in cyberembezzlement, funds are siphoned off electronically; [91] in cyberfraud, electronic communications transmit the false information that deceives the victim into parting with his property. [92] All of these are traditional theft accomplished by rather nontraditional means. One difference between online theft and "real world" theft is that cyberlarceny necessarily seems to be subsumed into cyberburglary, since it is difficult to imagine how a cyberthief can gain access to property for the purposes of carrying it away unless the thief illegally gains access to (breaks into) a computer system where the property is stored. [93]

38. The area in which cybertheft differs-or, more properly, can differ-from real world theft lies in the nature of the theft itself, e.g., the nature of the property that is taken. Real world theft is a zero sum offense, that is, an offense in which the sole possession and use of property is transferred from one person (the rightful owner) to another (the thief). [94] The same can be true of cybertheft: If a cyberthief, for example, hacks into a bank's computer system and transfers funds into accounts over which he maintains control, the thief now has those funds but the rightful owners of the funds no longer do. [95] That is one form of cybertheft, and this variety is, indeed, analogous to "real world" theft. There is, however, another form of cybertheft, one that is not a zero sum offense. [96] Assume, for example, that a cyberthief hacks into a computer system containing proprietary information that is owned by a business and that confers economic advantages on the possessor of that information (i.e., it has "value" in monetary terms). [97] The cyberthief could, of course, extract the information from the database containing the proprietary information and extract it, thereby depriving the owner of the information and achieving a classic, zero sum offense. [98] Instead of doing this, the cyberthief,

wanting to defer discovery of the theft for as long as possible, copies the information contained in the database; now, both the thief and the rightful owner possess the information. [99] Is this theft? It is not theft in classic terms, since the rightful owner still possesses the information. [100] It is, however, theft since the rightful owner has been deprived of some portion of the value of that information, the portion attributable to the rightful owner's formerly exclusive possession and use of the information. [101] One can characterize this type of theft as a dilution of the value of the information that has been copied by the cyberthief. [102]

39. This is an area that can be-and has been-problematic for applying traditional penal law to cybertheft. [103] That is, traditional penal laws usually do not incorporate the notion of non-zero sum thefts, in which a portion of the value of intangible property is taken but the rightful owner of the property is not completely deprived of its possession and use. [104] This is not, however, a flaw which requires the adoption of new, cybertheft-specific penal laws; this is a loophole which can be addressed by amending existing theft laws so that they do encompass the concept of stealing intangible property by making one or more copies of it. [105]

40. Forgery offenses can be dealt with more easily. The essence of forgery is the act of falsifying a document with the purpose of perpetrating a deception; in the past, the falsification was carried out on a paper document. [106] Cyberforgery simply introduces two new permutations, either of which can be adequately dealt with by amending extant forgery laws: (1) using computer technology to forge paper documents; or (2) using computer technology to forge electronic documents. This is not an area in which new, cybercrime-specific penal laws are required.[107]

41. Hacking is, as was noted above, rather more problematic. For the purposes of this discussion, hacking will be defined as the act of gaining unauthorized access to a computer system. [108] So defined, hacking is conceptually analogous to the traditional offense of trespass; trespass is the act of unlawfully gaining access to some "real world" physical space, such as another's property or a building owned by someone else.[109] The essence of the offense of hacking, like that of the offense of trespass, is the act of unlawfully entering into an area which is owned by someone else and which is not open to the general public. [110] One can, therefore, argue that there is no need to adopt penal laws which specifically target hacking, as the activity at issue could be penalized by amending "real world" trespass laws so they encompass the act of "breaking into" a computer system. [111] That is, of course, quite true; hacking could be prosecuted as a trespass if criminal trespass laws were modified so that they reach "virtual" trespass as well as "real world" trespass. [112] However, given the physical distinctions between the conduct that constitutes hacking and the distinct methods necessary to consummate a break-in into a computer system, it seems more reasonable to enact penal laws that specifically target hacking, as differentiated from "real world" trespassing.[113]

42. The same is true for "hactivism," which is less trespass-hacking and more a

type of attack on a web site, an attack motivated for political purposes.[114] While hacktivism could, perhaps, be analogized to "real world" vandalism, it, too, should be addressed by laws that specifically target this type of activity.[115] The rationale for adopting distinct laws to address this type of activity is in part based on the same notions that militate for adopting penal laws that specifically target hacking, i.e., the physical distinctions that exist between "real world" vandalism and hacktivism and the distinct methods needed to consummate an act of hacktivism.[116] Hacktivism can also be distinguished from "real world" vandalism in terms of the amount of damage each is likely to inflict; "real world" vandalism tends to inflict relatively minor damage on physical property, but hacktivism tends not only inflict damage on a web site per se but also to impair the web site proprietor's ability to carry out its lawful activities.[117] Also, one could analogize the activity encompassed under the rubric of hacktivism to the "hate crimes" that have been the target of specific penal legislation in a number of countries,[118] on the theory that both warrant the adoption of specific penal laws because each involves the victimization of a person or entity who has been chosen for socially intolerable reasons, e.g., expressing certain views (hactivism) or belonging to a specific racial, ethnic or cultural group (hate crimes).

43. There is, finally, another type of activity-i.e., "denial of service" attacks--which clearly requires the imposition of some type of criminal liability but which might evade prosecution under traditional penal laws. In a denial of service attack, the attacker floods a site with data, thereby overwhelming its capacity to respond and effectively shutting down traffic to that site.[119] Denial of service attacks can inflict great damage on online businesses, causing astronomical losses.[120] Since they do not cause physical damage to the attacked site(s), they could not be prosecuted as vandalism; since the attacker does not obtain services from the attacked site, they could not be prosecuted as a theft of services;[121] and since they do not actually involve penetration of the web site's computer systems, they could not be prosecuted as hacking, trespass or even burglary. The most logical approach is probably to adopt legislation that specifically targets these and other types of attacks on web sites, including the acts of disseminating viruses, worms and Trojan Horses.

Crimes Against Morality

44. So far, at least, computers do not seem to have given rise to the commission of new kinds of offenses against morality. Computer technology is simply being used as a tool to facilitate the commission of existing offenses against morality such as gambling, prostitution and the dissemination of obscene material.[122]

45. Therefore, while a country could adopt penal laws specifically targeting the use of computer technology to facilitate the commission of these and other offenses against morality,[123] that is not necessary as long as the country's existing penal laws are broad enough to encompass the activity at issue. If, for example, a country's penal laws make it a crime for a citizen of that country to gamble, then one who engaged in that activity can be prosecuted under those laws regardless of whether the gambling occurred in a "real world" casino or

online, in a virtual casino.[124] And the same is true if the country's laws prohibit the receipt, possession and/or dissemination of obscene materials; one who uses computer technology to do any of these things has violated those laws and can therefore be prosecuted under them. An offender may, of course, raise the issue of jurisdiction, claiming the offense was not "committed" in the prosecuting jurisdiction but elsewhere, either in "cyberspace" or in the country hosting the web site where the online casino is located or from which the obscene material originated.[125] Jurisdiction is a separate issue, one that goes not to the existence of penal laws but to their application; it is addressed in section IV, below.

46. The adequacy of a country's existing penal law will depend in part on the nature of the crime at issue: For the offenses discussed above-gambling and obscenitythe crime itself can be consummated online. This is not true for prostitution, at least not as prostitution has heretofore been defined. A country may, therefore, want to examine its prostitution and solicitation laws to ensure that they encompass using computer technology to facilitate the commission of the crime of prostitution.[126] And the same is true for other offenses against morality that can be facilitated by, but not committed via, computer technology.[127]

Crimes Against the Administration of Justice

47. Generally speaking, this is another area in which computer technology can be used as a tool to commit already-established crimes, but at least two new kinds of computer-facilitated activity that can undermine the administration of justice have emerged. The first paragraph below examines the use of computer technology to attack the administration of justice in traditional ways; the remainder of this section examine these new activities.

48. Computer technology can be used to obstruct justice in a number of traditional ways: generating false evidence or destroying electronic evidence; altering or deleting court records to erase criminal convictions or charges; threatening law enforcement officers and judges;[128] filing false reports of crimes; and shutting down crime-reporting systems such as 911 operations.[129] Also, someone can use it to impersonate a law enforcement officer or public official. [130] Here, as with many of the offenses discussed in sectionsection III(A)-(C), computer technology is simply a tool that is used to commit an existing crime. Jurisdictional issues aside, there should be no difficulty in prosecuting an offender under a country's existing obstruction of justice laws if, of course, those laws encompass the use of computer technology to commit the prohibited acts. If the laws in question define the offense(s) in generic terms, that will generally be sufficient;[131] with a few exceptions, it is not necessary that the penal law explicitly incorporate the use of computer technology to commit the offense.[132] That may, however, be necessary with regard to statutes that prohibit creating or altering evidence or public records because falsification of evidence statutes are often drafted so that they only encompass acts directed at "physical evidence."[133] Even if an evidence-tampering or record-tampering statute is phrased in more neutral terms,[134] it may still be advisable to amend the statute so that it explicitly encompasses electronic

records and the use of computer technology to alter or destroy records or data, in whatever form they are maintained.[135]

49. Now, as to the new activities: The administration of justice is, in every nation, a state monopoly; that is, countries do not allow citizens to take justice into their own hands, to engage in self-help when they have been the victims of a crime, because governments recognize that to allow this invites anarchy. Historically, those who have taken justice into their own hands-often known as "vigilantes"-were prosecuted for what they did; the prosecution typically takes the form of charging the vigilante not with the distinct offense of vigilantism but for the crimes he committed in the course of "doing justice." [136] A "real world" vigilante might, for example, be prosecuted for murder, for assault and/or for kidnapping, since, whatever the motivations responsible for these acts, he is not lawfully authorized to administer justice and cannot, therefore, use force against someone who has violated a nation's penal laws.

50. A comparable phenomenon-"cybervigilantism"-has emerged on the Internet. Frustrated by the actions of online offenders, some have either taken the law into their own hands or hired others to do so, to wreak vengeance for crimes (or other perceived wrongs) committed online, in the virtual world of cyberspace.[137] This is an issue nations need to examine: On the one hand, it may be possible to address cybervigilantism in the same way legal systems have addressed "real world" vigilantism, e.g., to prohibit and punish the discrete crimes those calling themselves vigilantes commit instead of trying to formulate a distinct offense of "cybervigilantism." On the other hand, since the tactics cybervigilantes exploit can bear little resemblance to the physical assaults their real world counterparts employ, it may be advisable for countries to adopt penal laws that specifically outlaw cybervigilantism. [138]

51. Obstruction of justice laws usually make it a crime to make threats against those charged with the administration of justice, including law enforcement officers.[139] A web site hosted on a server in the United States is raising new questions about what it means to "threaten" a law enforcement officer. The site lists the names, ranks, home addresses, home telephone numbers, salaries and Social Security numbers of police officers in fifteen different departments.[140] One police department has filed a civil suit attempting to shut down the web site, arguing that it jeopardizes the safety of the officers, since it provides information that could be used to retaliate against them.[141]

52. The issues raised by this web site are analogous to the issues raised by the cyberstalking variations discussed in section III(A), above. Here, as in the Alkhabaz and Dellapenta cases, there is no direct, "credible" threat communicated to a specific potential victim. Indeed, the information provided on this web site is in some senses far less "threatening" than the communications at issue in those two cases because it is content-neutral, e.g., it is simply a compilation of publicly-available information about a group of people selected because of the profession they all share. Of course, while the site dos not contain even fictive musings on inflicting harm to any of those who fall into this group, it can be characterized as an attempt to initiate a Dellapenta-style attack on one or more members of the group, e.g., to invite

others to take action against them. But even if one accepts this characterization, an effort to impose criminal liability for creating and maintaining such a web site necessitates considering, and resolving, the issue raised in the concluding paragraph of section III(A), above. And even if a legal system were to resolve these issues and decide to enact penal law imposing liability for a web site that posts personal information, how would the scope of this offense be defined? Would the offense be limited to posting information about law enforcement officers?[142] Would it also encompass other governmental officials? Would it include those engaged in other professions? Or would it resolve these issues by prohibit posting information about anyone? Finally, if a statute were to be adopted that imposed criminal liability for posting personal information about individuals falling into any or all of these categories, how would the imposition of liability be structured so as to avoid imposing liability on sites that "legitimately" offer certain information, e.g., telephone numbers, home addresses, e-mail addresses, etc.?[143]

Crimes Against the State

53. Crimes against the state can take a variety of forms, including acts specifically directed at destroying the viability of the state (e.g., treason and sabotage), [144] acts undertaken to weaken the effectiveness of the state (e.g., espionage, the internal dissemination of misinformation and propaganda, rioting),[145] acts targeting various state infrastructures (e.g., terrorism directed at transportation systems, economic systems, public utilities, medical systems, etc.),[146] acts taken to undermine the state's fiscal stability (e.g., counterfeiting), [147] and the like. Crimes against religion can also be included in this category of offenses. [148]

54. This category is made up of offenses the general contours of which have been clearly established, which means computer technology will become at most a tool used to commit these crimes. Treason, for example, is generally defined as actions by one who owes a duty of allegiance to a country but who levies war against that country or gives aid and comfort to its enemies. [149] Computer technology can of course be applied to this end; a traitor could, for example, break into a national computer system, extract vital national secrets and give those secrets to an enemy nation. [150] By the same token, computer technology can be used to attack essential infrastructures, [151] weaken a country's ability to respond to attacks from abroad, [152] and/or undermine its fiscal stability. [153] But each of these scenarios represents merely the application of new technology to achieve ends that have traditionally been prohibited by penal laws, since nations have long recognized that they cannot tolerate actions taken to undermine their very existence. Nations may want to reassess these laws to ensure that they explicitly encompass the use of computer technology to this end, but this is not an area in which there is a need to develop entirely new offenses, e.g., entirely new penal laws.[154]

Procedural Law: Some General Issues

55. As section I explained, the primary focus of the article is on penal laws because the generic consistency one encounters in penal laws permits a broad

analysis of how these laws can be adapted to deal with cybercrime. Such an analysis is more problematic when one turns to procedural law, since there is much more variation among nations in this area. Notwithstanding that, it is important at least to note how procedural law may need to be revised to facilitate the investigation and apprehension of cybercriminals. After all, a country can have a comprehensive penal code that reaches every known variety of cybercrime but still be unable to prosecute cybercriminals because of gaps in its procedural law.

56. Cybercrime is often transnational crime, which raises the issue of jurisdiction to prosecute the offender. [155] Countries must examine their procedural law and, if necessary, amend it so they can legitimately exercise jurisdiction over cybercrimes.[156] Traditionally, jurisdiction has been equated with territory, with the scope of a country's being defined by the limits of its territorial boundaries. [157] This territorial notion of jurisdiction to prosecute becomes problematic when dealing with cybercriminals. Determining where a cybercrime was "committed" can be difficult, since the perpetrator and the victim can be located in different countries and since the perpetrator may utilize computer systems in several countries in the course of attacking the victim. [158] One approach to this problem is to broaden the territorial notion of jurisdiction to prosecute so that it allows the nation to prosecute whenever the offender's conduct occurred in whole or in part in the prosecuting nation's territory.[159] This approach would, for example, give the country jurisdiction to prosecute a cybercriminal (a) when both the victim(s) and the perpetrator were located in the country at the time the crime was committed and the perpetrator utilized computer technology located in that country;[160] (b) when either the victim or the perpetrator was located in that country during the commission of the crime;[161] and/or (c) when any part of the crime was committed, planned or facilitated in that country. [162] Finally, countries can impose their own penal law on their citizens when the citizens are abroad, which means that a country could prosecute one of its nationals for committing a cybercrime even though the actual commission of the offense was carried out in another country and did not have harmful effects on people or property located within the prosecuting jurisdiction. [163]

57. Because it exploits technology, cybercrime can create problems for investigators who must obey procedural rules crafted to deal with the investigation of crime in the "real world" of physical space, not the virtual world of cyberspace. Procedural law may, for example, only provide authorization to search for and seize tangible evidence.[164] Since the prosecution of cybercrimes usually requires collecting and analyzing intangible evidence, this omission can be a serious problem for investigators.[165] Countries must, therefore, evaluate their procedural law governing evidence-collecting and -analysis and amend it, as necessary, so that it does not suffer from this and other limitations.[166]

Conclusion

58. Cybercrimes raise new issues for legal systems. As the world's experience with

the "Love bug" virus demonstrated, cybercriminals can exploit gaps in a nation's penal and procedural laws and thereby evade prosecution.

59. This exploitation takes two forms. On the one hand, the permeability of national boundaries resulting from the Internet allows an offender situated in one country to perpetrate crimes in other countries; the remote offender may be able to operate with impunity, especially if the country in which he is located does not have penal laws which reach his conduct. This lack of adequate penal laws will prevent the offender's being prosecuted in his own country (assuming he did, in fact, commit offenses there as well), will prevent his being extradited to the countries he has victimized and can hamper law enforcement's ability to investigate and apprehend him. The world's experience with the "love bug" virus demonstrated all this: Onel de Guzman, suspected of disseminating the virus, could not be prosecuted in the Philippines because the Philippines' penal laws did not prohibit creating and disseminating a virus; since what he did was not a crime in his home country, he could not be extradited to countries in which it was a crime; and investigators found it difficult to get search warrants to investigate the episode because the dissemination of the virus was not a local crime. This scenario is intolerable, and not just because it is embarrassing for the offender's home country and frustrating for the countries whose citizens have been victimized; it is intolerable because it can so easily be repeated unless countries recognize that cybercrimes transcend borders and cannot, therefore, be treated as simply a local problem. One nation's inadequate penal laws can result in the victimization of citizens of other countries, countries which have tried to protect their citizens by adopting laws adequate to prohibit the conduct at issue.

60. But it is not only remote cyberoffenders who exploit gaps in penal laws. A cybercriminal can take advantage of such gaps to commit crimes against individuals and/or businesses in his own country, knowing he cannot be prosecuted for what he does.

61. The obvious solution to both forms of exploitation is for countries to ensure that their penal and procedural laws are adequate to permit the investigation and prosecution of cybercriminals. Indeed, this is a central feature of two conventions that have been drafted to deal with cybercrime. The Council of Europe's Draft Convention on Cyber-Crime seeks "to improve the means to prevent and suppress computer- or computer - related crime by establishing a common minimum standard of relevant offences." [167] Parties to the Convention would agree to adopt penal legislation addressing five types of cybercrimes: (1) illegal interception of and/or interference with computer data, illegal access to and/or interference with computer systems, and the misuse of devices to commit any of these offenses; (2) computer-related forgery and fraud; (3) child pornography; (4) the infringement of copyright and related rights; and (5) provisions governing the imposition of aiding and abetting and corporate liability.[168] They would also agree to adopt legislation guaranteeing the availability of certain procedures used to investigate cybercrime and apprehend cybercriminals.[169] The convention proposed by the Center for International Security and Cooperation (CISAC) has similar

provisions, although it differs in some respects.[170] As to the adoption of penal laws, parties to the CISAC Convention would agree to adopt laws prohibiting the following: illegal entry into a computer system; manipulating data to affect the functioning of a computer system and/or to cause "substantial damage" to persons or property; interfering with authentication or tamper-detection mechanisms; manufacturing or distributing a device used to commit any offense within the scope of the Convention; and using computer technology to engage in activity outlawed by a list of treaties.[171] Like the Council of Europe's Draft Convention, the CISAC Convention addresses liability for aiding and abetting the commission of the identified cybercrimes and requires that signatories adopt procedural law governing mutual legal assistance in investigating cybercrimes.[172] Both the Council of Europe and CISAC Conventions consign the drafting of the legislation they respectively require to the parties who execute the convention; the architects of the Conventions recognized that nations have their own approaches to defining offenses and specifying the methods that can be used to investigate crimes.[173]

62. These Conventions are estimable attempts to begin the process of establishing consistency in the cybercrime laws of the various nations. But regardless of whether a country executes, or plans to execute, one of these Conventions, it should conduct an audit of its penal and procedural laws to determine whether they provide police and prosecutors with the tools they need to pursue cybercriminals. This may mean adding new laws, amending existing laws and/or doing nothing if existing laws are adequate for this purpose. There is no need to adopt cybercrime-specific laws if a nation's existing laws are adequate or can be made adequate with some amendments; indeed, there are good reasons not to adopt cybercrime-specific laws when either of these conditions exists. For one thing, a country's law enforcement personnel will be familiar with the laws that already exist, having used them in the past; the interpretation of those laws will be clear and their legality under governing national principles will have been tested and established. For another, those drafting cybercrime-specific laws sometimes tie the legislation to existing technology, which means it can quickly become outmoded.[174] And, finally, duplicative laws-e.g., having cybercrime-specific offenses that are analogues of "real world" offenses-can sometimes be exploited by defendants, who can argue that they have been charged under the wrong statutory scheme and/or that the existence of a set of parallel laws somehow establishes that one legislative schema is flawed in some material and significant respect. [175]

63. There may, or may not, be "virtual crimes" that will require new legislative responses,[176] but the prudent approach is to take a conservative tack in dealing with technologically-facilitated offenses, employing existing law whenever possible. One expert in this area hypothesizes the emergence of "computer crime in a box," e.g., of software programs that will "perform completed crimes including selection of victims, illegal acts, conversion to gain, and erasure of all evidence."[177] While the hypothesized scenario might seem to require the adoption of new law, it could, in fact, be substantially addressed by using tried and true legal principles.[178]

64. Start with the premise that the software will be used to commit "crimes." What form might these crimes take? Since human motivation is the driver of any crime, and since the range of motives responsible for crime has been well established, it is almost certain that the "crimes" will fall into a known category, e.g., crimes against persons, crimes against property, crimes against morality, crimes against the administration of justice or crimes against the state. So the penal law will no doubt have addressed the underlying offense, which means that the purchaser and user of the software can be prosecuted for that offense.[179] The purveyor of the software can be prosecuted using other well-established legal principles: He can be prosecuted for aiding and abetting the underlying offense, since he provided the offender with the tools used to commit that offense.[180] The purveyor could also be prosecuted for conspiringwith the purchaser of the software, with the designer of the software and/or with anyone else involved in its dissemination-to commit the underlying offense.[181] And holding the purveyor liable under these theories is a just result, one which reflects the measure of harm he actually inflicted on the victims and on the legal system in which his actions occurred; he did not actually use the software to engage in the prohibited activity, so it is reasonable to apportion liability differently between the purveyor and the person who did engage in that activity.

65. Legislative responses to cybercrime should be both rigorous and conservative. They should be rigorous in evaluating the legal system's EXISTING ability to deal with cybercrime, but they should be conservative in taking steps to improve that ability.

Notes

[1] See Part II, infra.

[2] See Part II, infra.

[3] See Part II, infra.

[4] See Part III & IV, infra.

[5] See Part II, infra.

[6] Fast-spreading Virus Hits U.S., Asia, Europe, USAToday (June 7, 2000), http://www.usatoday.com/life/cyber/tech/cth837.htm.

[7] See, e.g., Corporate Systems Hard-Hit by Virus, USA Today (June 7, 2000), http://www.usatoday.com/life/cyber/tech/cth839.htm.

[8] See, e.g., Philipplines' Laws Complicate Virus Case, USAToday (June 7, 2000), http://www.usatoday.com/life/cyber/tech/cth879.htm ("Finally, . . . a judge agreed to issue a warrant under a 1998 law regulating the use of 'access devices' such as credit cards or equipment to obtain money, goods or services").

[9] See, e.g., Charges Dropped Against Love bug Suspect, USAToday, (August 21, 2000), http://www.usatoday.com/life/cyber/tech/cti418.htm. The theft and fraud charges were apparently abased on the fact that the "love bug" was designed to steal computer passwords. The charging premise seems to have been that the virus was intended to steal "property"-i.e., passwords-and use

them to commit fraud-i.e., to obtain computer services, and perhaps other property, by deception. See, e.g., Love bug Virus May Be Accident, USAToday (June 7, 2000) (http://www.usatoday.com/life/cyber/tech/cth894.htm (de Guzman's thesis project was a computer program that was designed to steal passwords; the thesis project was rejected because it was designed to commit theft).

[10] See, e.g., Charges Dropped Against Love bug Suspect, USAToday, (August 21, 2000), http://www.usatoday.com/life/cyber/tech/cti418.htm.

[11] See, e.g., David Noack, "Love bug" Damage Worldwide: $10 Billion, apbnews.com, http://www.apbnews.com/newscenter/internetcrime/2000/05/08/lovebug_impact0508_01 .html; Dirk Beveridge, Student Says He May Have Sent Out "Love bug" Virus Accidentally, The Detroit News (May 12, 2000), http://detnews.com/2000/technology/0005/15/-54297.htm.

[12] See, e.g., David Noack, "Love bug" Damage Worldwide: $10 Billion, apbnews.com, http://www.apbnews.com/newscenter/internetcrime/2000/05/08/lovebug_impact0508_01 .html; Dirk Beveridge, Student Says He May Have Sent Out "Love bug" Virus Accidentally, The Detroit News (May 12, 2000), http://detnews.com/2000/technology/0005/15/-54297.htm.

[13] See, e.g., "Love bug" Prompts New Philippine Law, USAToday (June 14, 2000), http://www.usatoday.com/life/cyber/tech/cti095.htm (under the new law, hackers and those who spread computer viruses can be fined a minimum of $2,350 and a maximum "commensurate" with the damage caused, and can be imprisoned for up to three years). See also Republic of the Philippines, Eleventh Congress - Second Regular Session, Republic Act No. 8792, Part V section 33, http://www.mcconnellinternational.com/services/country/philippines.pdf.

[14] See, e.g., "Love bug" Prompts New Philippine Law, USAToday (June 14, 2000), http://www.usatoday.com/life/cyber/tech/cti095.htm.

[15] See, e.g., Philipplines' Laws Complicate Virus Case, USAToday (June 7, 2000), http://www.usatoday.com/life/cyber/tech/cth879.htm: `This is a new type of crime and the law applicable is not so clear,' said [Philippines National Bureau of Investigation] director Federico Opinion, who admitted that his own office has no computers, and whose agency was assisted by the FBI in the so-called Love bug case.

Scores of nations, especially in the developing world, lack laws governing cyberspace crimes and are woefully short on the computer-savvy investigators and technology required to go after sophisticated hackers.

'The scary thing about the Internet is that somebody with a computer in a jurisdiction where there are no cybercrime laws can get on and wreak havoc around the rest of the world,"said Susan Brenner, a cybercrime expert at The University of Dayton Law School in Ohio.

Thirty-seven countries now have statutes dealing with "unauthorized access" to computers and computer systems, according to a list compiled by Stein Schjolberg, a Norwegian judge active in cyberjurisprudence.

But the laws are anything but uniform and there are no international treaties governing cybercrime. The European Union released a draft treaty last week, said Brenner, adding that it would not be approved until next year at the earliest.

In the meantime, the lack of global legal standards for combating malicious hackers is 'going to cause delays in cooperation, with investigators floundering around as to what they should try to do,' said John F. Murphy, a Villanova University law professor who specializes in international terrorism. . . .

Even with such laws, locating and successfully prosecuting cyber culprits 'is like tracing vapor'

because skilled hackers can make it difficult to establish their identities on the Internet, said Philippine law professor Josephine Victoria T. Yam.

The Net's global nature can even frustrate law enforcement cooperation among countries that have cybercrime statutes because of their lack of uniformity.

There is, for example, great potential for disputes regarding admissibility of electronic evidence, which is weighed differently in different countries.

There are also disputes over which country should have jurisdiction over an offender - the hacker's home country or those of his victims.

Take the case of the Love bug virus, which struck millions of computers worldwide when it was unleashed Thursday, causing hundreds of millions of dollars in damage.

'Is the crime the creating and setting loose of the thing or is the crime the damage committed and where?,' posed Brenner, the U.S. cybercrime expert. 'In that case we have millions of cases of damage.'

The United States has not said whether it would seek the extradition of the Love bug virus authors. But if Washington were to do so, the lack of Philippine cybercrime law could be an impediment.

Although the United States and the Philippines have an extradition treaty, Philippine law requires that laws exist in both countries recognizing a given offense.

[16] A recent study points out that countries which do not have adequate cybercrime laws "will become less able to compete in the new economy" because "[a]s cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network." McConnell International, Cyber Crime and Punishment ("Overview"), http://www.mcconnellinternational.com/services/cybercrime.htm.

[17] See, e.g., Student Calls "Love bug" Virus an Accident, Muzi News (May 11, 2000), http://news.muzi.com/ll/english/68369.shtml; Love bug Suspect Suggests It Was "Accidental", apbnews.com (May 11, 2000), http://www.apbnews.com/newscenter/internetcrime/2000/05/11/lovebug0511_01.html.

[18] See, e.g., United States v. Baker, 1997 Fed. App. 0036P (Sixth Circuit Court of Appeals 1997), http://laws.lp.findlaw.com/6th/970036p.html (U.S. federal courts of appeals upheld dismissal of charges against defendant who posted descriptions of his raping, torturing and killing woman online because provisions of federal criminal statute did not encompass his actions). The Baker case is discussed in Section III, infra.

[19] See, e.g., Lynn Burke, Love bug Case Dead in Manila, Wired News (August 21, 2000), http://www.wired.com/news/print/0,1294,38342,00.html (in the aftermath of the "love bug" episode, U.S. prosecutor quoted as stating that "`[a]s long as there are governments that don't take these crimes seriously, it's going to be very difficult for other countries to really protect their computers'").

[20] See, e.g., Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism ("Why a Multilateral Convention"), http://www.oas.org/juridico/english/monograph.htm.

[21] Some reports indicated that many people "in the Philippines seem[ed] to care little about the ["love bug"] virus, which posed few problems in the relatively uncomputerized country but stirred cyber chaos in the wealthy West." See, e.g., Student Calls "Love bug" Virus an Accident, Muzi

News (May 11, 2000), http://news.muzi.com/ll/english/68369.shtml. See also Love bug Suspect Suggests It Was "Accidental", apbnews.com (May 11, 2000), http://www.apbnews.com/newscenter/internetcrime/2000/05/11/lovebug0511_01.html (noting that the speaker of the Philippine House of Representatives described the suspect as a "misguided genius" and said the dissemination of the virus showed "that the Philippines possesses world-class information technology skills").

[22] See, e.g., Lynn Burke, Love bug Case Dead in Manila, Wired News (August 21, 2000), http://www.wired.com/news/print/0,1294,38342,00.html (since Philippine law did not outlaw the creation and dissemination of viruses, the "love bug" suspect could not be extradited to countries with such laws, like the United State of America). See also Extradition Treaty Between The Government of Belize and the Government of The United States of America, Article 1, http://www.belize.gov.bz/features/treaty/welcome.html#1 ("The Contracting States agree to extradite to each other, pursuant to the provisions of this Treaty, persons sought for prosecution or convicted of an extraditable offense by the authorities in the Requesting State").

An offense shall be an extraditable offense if it falls within any of the descriptions listed in the Schedule annexed to this Treaty, which is an integral part of the Treaty, or any other offense, provided that in either case the offense is punishable under the laws in both Contracting States by deprivation of liberty for a period of miore than one year or by a more severe penalty.

Extradition Treaty Between The Government of Belize and the Government of The United States of America, Article 2(1), http://www.belize.gov.bz/features/treaty/welcome.html#1. See generally United States v. Lui, http://www.law.emory.edu/1circuit/mar97/97-1084.01a.html (reviewing U.S. extradition law).

[23] See generally Council of Europe, Draft Convention on Cyber-Crime (Draft No. 25 Rev. 5), http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm (noting need for cooperation among nations to mount an "effective fight against cyber-crime").

[24] See, e.g., McConnell International, Cyber Crime and Punishment ("What's Different About Cyber Crime?"), http://www.mcconnellinternational.com/services/cybercrime.htm:

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

[25] See, e.g., U.S. Wants More Cybercrime Laws, Wired News (July 26, 2000), http://www.wired.com/news/politics/0,1283,37809,00.html:

More than 100 countries do not have the laws to deal with computer-related crime, undercutting efforts to battle a growing international threat, law enforcement officials said on Wednesday. `Currently, at least 60 percent of INTERPOL membership lacks the appropriate legislation to deal with Internet/computer-related crime,' Edgar Adamson of the U.S. Customs Service told a House of Representatives panel. Adamson heads the U.S. National Central Bureau, which coordinates U.S. ties to INTERPOL, the global police alliance facilitating cooperation among 178 member nations. In testimony prepared for the Subcommittee on Government Management, Information and Technology, Adamson said the border-hopping nature of cyber crime showed the need for international law-enforcement cooperation `has never been greater.' At issue is garden-variety crime facilitated by new technology such as child pornography, pedophilia, identity theft, and credit-card fraud as well as viruses and other malicious code like the `denial of service' attacks that blocked access to major commercial websites in February.

[26] McConnell International, Cyber Crime and Punishment ("The Cyber Crime Laws of Nations"), http://www.mcconnellinternational.com/services/cybercrime.htm. For a list of the 52 countries, see McConnell International, Cyber Crime and Punishment note 4, http://www.mcconnellinternational.com/services/cybercrime.htm.

[27] See also Stein Schj¿lberg, The Legal Framework - Unauthorized Access to Computer Systems; Penal Legislation in 37 Countries (collecting cybercrime- specific legislation adopted in various countries), http://www.mossbyrett.of.no/info/legal.html#COUNTRIES.

[28] See, e.g., McConnell International, Cyber Crime and Punishment ("The Cyber Crime Laws of Nations"), http://www.mcconnellinternational.com/services/cybercrime.htm. This study focused on data-related crimes (interception, modification and theft), network- related crimes (interference and sabotage), access crimes (hacking and virus distribution) and "associated computer-related crimes" (fraud, forgery and aiding and abetting computer criminals).

[29] See, e.g., McConnell International, Cyber Crime and Punishment ("The Cyber Crime Laws of Nations"), http://www.mcconnellinternational.com/services/cybercrime.htm. This study did consider whether countries had amended their existing penal laws to "extend" them into cyberspace; and the report notes that law enforcement officials in some countries, Canada being an example, believe their existing laws provide adequate protection against certain types of cybercrimes, such as fraud, forgery and aiding and abetting cybercrime. See, e.g., McConnell International, Cyber Crime and Punishment ("The Cyber Crime Laws of Nations"), http://www.mcconnellinternational.com/services/cybercrime.htm. The authors of the report do not, however, seem to believe traditional penal law is adequate for this purpose: In the conclusion, the report explains that "[d]espite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber crimes." See McConnell International, Cyber Crime and Punishment ("Conclusions"), http://www.mcconnellinternational.com/services/cybercrime.htm. The report describes these laws as "archaic" and suggests they are inadequate for this purpose. See McConnell International, Cyber Crime and Punishment ("Conclusions"), http://www.mcconnellinternational.com/services/cybercrime.htm.

[30] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[31] These categories are a distillation of the general categories one encounters in penal codes around the world. See, e.g., Criminal Code of Canada, http://laws.justice.gc.ca/en/C-46/index.html; Criminal Law of the People's Republic of China, http://www.qis.net/chinalaw/prclaw60.htm; New South Wales, Crimes Act 1900, http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/; Revised Penal Code of the Philippines, Book Two, http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm. See also American Law Institute, Model Penal Code, http://www.ali.org.

[32] See, e.g., 1999 Revision of the Model State Computer Crimes Code, http://www.cybercrimes.net/99MSCCC/99MSCCCMain.html.

[33] See, e.g., German Law Archive, German Penal Code section 211, http://www.iuscomp.org/gla/; Swedish Penal Code, Part 2 - Chapter 3 section 1, http://wings.buffalo.edu/law/bclc/sweden.pdf.

[34] See, e.g., German Law Archive, German Penal Code sectionsection 223-226, http://www.iuscomp.org/gla/.

[35] See, e.g., Criminal Code of Canada, Part VIII ("Offenses Against the Person and Reputation"), http://laws.justice.gc.ca/en/C-46/index.html; Criminal Law of the People's Republic of China, Part II - Chapter IV, http://www.qis.net/chinalaw/prclaw60.htm; Revised Penal Code of the Philippines, Book Two, Title Eight,

http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm

[36] See, e.g., Criminal Code of Canada, Part V, http://laws.justice.gc.ca/en/C-46/index.html; Criminal Law of the People's Republic of China, Chapter IV, http://www.qis.net/chinalaw/prclaw60.htm; New South Wales, Crimes Act 1900, Part 3, http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/; Revised Penal Code of the Philippines, Book Two, Title Eleven, http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm; Swedish Penal Code, Part 2 - Chapter 6 section 1, http://wings.buffalo.edu/law/bclc/sweden.pdf.

[37] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[38] See, e.g., 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.01.1, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.01.1.html:

For example, an individual hacks into an industry's computer, say General Motor's computer. The individual then programs the computer so that the 2001 Chevy Blazer is modified. The modification is that the brakes will fail on every 10th Blazer produced after it has been driven for 5002 miles. If a person who buys a Chevy Blazer and then dies because the brakes failed due to the modification of the design made by the individual hacker, then the individual is guilty of . . . murder . . . .

There are anecdotal reports that this has occurred, but the stories so far seem to be apocryphal. See, e.g., David L. Carter, Computer Crime Categories: How Computer Criminals Operate, http://www.lectlaw.com/files/cri14.htm; Corporate Crime, http://www.williamsinference.com/2414crime.htm. Hackers have, however, gained entry to hospital records. See, e.g., Kevin Poulsen, Hospital Records Hacked Hard, The Register (December 17, 2000), http://www.theregister.co.uk/content/6/15285.html ("A sophisticated hacker took command of large portions of the University of Washington Medical Centre's internal network earlier this year and downloaded computerized admissions records for four thousand heart patients").

[39] Extradition may, of course, be impeded by other issues, such as the extraditing nation's discomfort with the penalty that can be imposed by the nation seeking to prosecute the perpetrator. See, e.g., Canada Bars Death- Penalty Extradition to U.S., The Irish Times (April 22, 2001), http://www.ireland.com/newspaper/breaking/2001/0215/breaking82.htm. But issues such as this arise without regard to whether the commission of the offense involved the use of a computer and so implicated the notion of "cybercrime."

[40] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[41] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[42] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/. See also 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.01.1, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.01.1.html ("Computer Homicide is designated as a null section because the drafters of the Code feel that the existing law is sufficient to cover homicides which occur via the computer").

[43] See generally 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.01.1, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.01.1.html (hypothesizing product alteration to effect murder).

[44] See, e.g., Texas Penal Code section 22.07, http://www.bakers-legal-pages.com/pc/2207.htm (offense to threaten to commit any offense involving violence to person or property with the intent to place any person in fear of imminent serious bodily injury).

[45] See, e.g., State v. Gallicio, 129 So. 541 (La. 1930) (conviction for using telephone to transmit threat to "kill, maim, wound and murder" victim over telephone upheld). See also People v. Daly, 154 Misc. 149, 276 N.Y.S. 583 (1935); People ex rel. Gannon v. McAdoo, 117 A.D. 438, 102 N.Y.S. 656 (1907).

[46] See, e.g., People v. Munn, 688 N.Y.S. 2d 384, 386 (N.Y. City Criminal Court 1999):

I find . . . that the allegations are sufficient to establish the elements of the charge of aggravated harassment in the second degree and that Penal Law section 240.30(1) may be construed to prohibit harassing and threatening messages sent to individuals over the Internet. This is true even though the law was originally written in 1965 and then revised in 1969, before Internet communication was envisioned. The present language of the statute is broad enough as it stands to prohibit this type of computer-generated harassing communication.

[47] See generally 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.01.1, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.01.1.html (hypothesizing product alteration to effect murder).

[48] See 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.02.2, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.02.2html (discussing this scenario and the challenges it poses for traditional law).

[49] 18 U.S. Code section 875(a) provides as follows:

(a) Whoever transmits in interstate or foreign commerce any communication containing any demand or request for a ransom or reward for the release of any kidnapped person, shall be fined under this title or imprisoned not more than twenty years, or both. (b) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than twenty years, or both. (c) Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both. (d) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

[50] 104 F.3d 1492, 1997 Fed. App. 0036P (Sixth Circuit Court of Appeals 1997), http://laws.lp.findlaw.com/6th/970036p.html.

[51] See 104 F.3d at 1495-1496, 1997 Fed. App. 0036P, http://laws.lp.findlaw.com/6th/970036p.html.

[52] See 104 F.3d at 1498, 1997 Fed. App. 0036P, http://laws.lp.findlaw.com/6th/970036p.html (Krupansky, J., dissenting):

By November 1994, Baker's sadistic stories attracted the attention of an individual who called himself `Arthur Gonda,= a Usenet service subscriber residing in Ontario, Canada, who apparently shared similarly misdirected proclivities. Baker and Gonda subsequently exchanged at least 41 private computerized electronic mail ("e-mail") communications between November 29, 1994 and January 25, 1995. Concurrently, Baker continued to distribute violent sordid tales on the

electronic bulletin board. On January 9, 1995, Baker brazenly disseminated publicly, via the electronic bulletin board, a depraved torture- and-snuff story in which the victim shared the name of a female classmate of Baker's referred to below as "Jane Doe" . . . This imprudent act triggered notification of the University of Michigan authorities by an alarmed citizen on January 18, 1995. On the following day, Baker admitted to a University of Michigan investigator that he had authored the story and published it on the Internet.

[53] See 104 F.3d at 1493, 1997 Fed. App. 0036P, http://laws.lp.findlaw.com/6th/970036p.html.

[54] See 104 F.3d at 1493, 1997 Fed. App. 0036P, http://laws.lp.findlaw.com/6th/970036p.html.

[55] See 104 F.3d at 1497, 1997 Fed. App. 0036P, http://laws.lp.findlaw.com/6th/970036p.html:

Accordingly, to achieve the intent of Congress, we hold that, to constitute "a communication containing a threat" under Section 875(c), a communication must be such that a reasonable person (1) would take the statement as a serious expression of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reus). . . .Applying our interpretation of the statute to the facts before us, we conclude that the communications between Baker and Gonda do not constitute "communications containing a threat" under Section 875(c). Even if a reasonable person would take the communications between Baker and Gonda as serious expressions of an intention to inflict bodily harm, no reasonable person would perceive such communications as being conveyed to effect some change or achieve some goal through intimidation. Quite the opposite, Baker and Gonda apparently sent e- mail messages to each other in an attempt to foster a friendship based on shared sexual fantasies.

See also 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.02.2, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.02.2html (discussing this scenario and the challenges it poses for traditional law).

[56] See, e.g., 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.02.2, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.02.2html:

[One scenario arose in] . . . Will County, Chicago. In this case, an individual proficient with the use of a computer used the Internet to post a child's (or adult's) name and telephone number on sexual explicit Internet sites. This posting invited visitors to call and inquire about the named individual, who was a child. As a result, the named individual was subjected to consistent, harassing and possibly sexual explicit telephone calls every day of the week, at any and all hours. The repeated inquiries caused the recipient of the calls and/or messages to become fearful for his/her safety and the safety of their family. The Boehle family decided that they had to move outside of Will County in order to protect their daughter, who was the subject of the postings, telephone calls and messages, from any potential harm they feared might occur as a result of such harassment.

(footnotes omitted).

[57] See, e.g., U.S. Department of Justice, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, http://www.usdoj.gov:80/criminal/cybercrime/cyberstalking.htm.

[58] See, e.g., U.S. Department of Justice, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, http://www.usdoj.gov:80/criminal/cybercrime/cyberstalking.htm.

[59] See, e.g., Cyberstalking Law Invoked, Wired News (January 25, 1999), http://www.wired.com/news/politics/0,1283,17504,00.html.

[60] See, e.g., Feds Find Dangerous Cyberstalking Hard to Prevent, cnn.com (June 12, 2000), http://europe.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/.

[61] See California Penal Code section 646.9(a), http://caselaw.lp.findlaw.com/cacodes/pen/639-653.1.html:

Any person who willfully, maliciously, and repeatedly follows or harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family, is guilty of the crime of stalking, punishable by imprisonment in a county jail for not more than one year or by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment, or by imprisonment in the state prison.

Note that this statute does require a "credible threat." The statutory definition of a "credible threat" is, however, broad enough to encompass Dellapenta's conduct. See California Penal Code section 646.9(g), http://caselaw.lp.findlaw.com/cacodes/pen/639-653.1.html ("`"credible threat' means a verbal or written threat, including that performed through the use of an electronic communication device, or a threat implied by a pattern of conduct or a combination of verbal, written, or electronically communicated statements and conduct made with the intent to place the person that is the target of the threat in reasonable fear for his or her safety or the safety of his or her family and made with theapparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for his or her safety or the safety of his or her family").

[62] See, e.g., Feds Find Dangerous Cyberstalking Hard to Prevent, cnn.com (June 12, 2000), http://europe.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/. See also Cyberstalking: The Cases (Randi Barber), citing State v. Dellapenta (Los Angeles Superior Court 1999), http://www.unc.edu/courses/law357c/cyberprojects/spring00/cyberstalking/cyberstalk/cases.html#barber.

[63] See, e.g., Feds Find Dangerous Cyberstalking Hard to Prevent, cnn.com (June 12, 2000), http://europe.cnn.com/2000/TECH/computing/06/12/cyberstalkers.idg/.

[64] See, e.g., Cyberstalking: The Cases, http://www.unc.edu/courses/law357c/cyberprojects/spring00/cyberstalking/cyberstalk/cases.html.

[65] See, e.g., 1999 Revision of the Model State Computer Crimes Code, Commentary to section 2.02.2, http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.02.2html.

[66] For a discussion of the distinctions between cyberstalking and online harassment, see, e.g., 1999 Revision of the Model State Computer Crimes Code, sectionsection 2.02 & 2.03, http://www.cybercrimes.net/99MSCCC/99MSCCCMain.html.

[67] See, e.g., Cyberstalking: The Cases, http://www.unc.edu/courses/law357c/cyberprojects/spring00/cyberstalking/cyberstalk/cases.html.

[68] Cyberstalking and online harassment can have a sexual focus or a non-sexual focus. See, e.g., 1999 Revision of the Model State Computer Crimes Code, sectionsection 2.02 & 2.03, http://www.cybercrimes.net/99MSCCC/99MSCCCMain.html. The discussion above tends to assume non-sexual cyberstalking and/or online harassment, simply to provide a contrast to the issues raised by specifically sexual offenses such as rape.

[69] See Julian Dibbell, A Rape in Cyberspace, http://www.humanities.uci.edu/mposter/syllabi/readings/rape.html.

[70] See, e.g., 1999 Revision of the Model State Computer Crimes Code, section 3.04.1, http://cybercrimes.net/99MSCCC/MSCCC/Article3/3.04.1.html.

[71] See, e.g., 1999 Revision of the Model State Computer Crimes Code, section 3.04.1, http://cybercrimes.net/99MSCCC/MSCCC/Article3/3.04.1.html.

[72] See, e.g., 1999 Revision of the Model State Computer Crimes Code, section 3.04.1, http://cybercrimes.net/99MSCCC/MSCCC/Article3/3.04.1.html.

[73] See, e.g., 1999 Revision of the Model State Computer Crimes Code, section 3.04.1, http://cybercrimes.net/99MSCCC/MSCCC/Article3/3.04.1.html.

[74] To avoid copyright issues, we will assume that the video is entirely the perpetrator's creation, using computer technology and, perhaps, live actors.

[75] Relying on civil remedies is likely to be inadequate, as this case illustrates:

Jayne Hitchcock's ordeal started after she exposed an Internet scam being run by a group of people calling themselves the Woodside Literary Agency. Jayne was suddenly the target of an elaborate smear campaign designed to intimidate, harass, and belittle her. First the agency launched a series of emailbombs (to her home, to her place of work at the University of Maryland, and to her husband Chris' email account). Then, the harassers forged posts in her name to hundreds of newsgroups. The posts indicated that Jayne was interested in having people call or stop by her house to share their sexual fantasies with her. Her home address and phone number were included. Jayne described her emotional state by saying: "I felt like someone had broken into my house, touched all of my things, didn't take anything and left -- I felt violated and scared for my life."

Jayne attempted to get help from the police. She contacted her local police department, the police commissioner, even the FBI. No one she spoke to could help. Eventually, Jayne decided she would take care of the problem herself. She and a group of her friends and family tracked down the stalkers themselves.

Since her harassers were not subject to criminal prosecution, Jayne filed several civil suits (one for $10 million) that are still pending. After the civil suits were filed, the harassment worsened, and Jayne was forced to go to therapy to deal with the problems it was causing her. In order to avoid her harassers, Jayne and her family relocated to another state and had their names removed from public records. The harassment stopped for only a short time. Jayne is still the target of Internet harassment.

Cyberstalking: The Cases, http://www.unc.edu/courses/law357c/cyberprojects/spring00/cyberstalking/cyberstalk/cases.html#hitchcock.

[76] See Free Speech Coalition v. Reno, 198 F.3d 1083, 1089 (9th Cir. 1999), certiorari granted, 121 S.Ct. 826 (January 22, 2001):

The Child Pornography Prevention Act of 1996 expanded the law to combat the use of computer technology to produce pornography containing images that look like children. The new law sought to stifle the use of technology for evil purposes. This of course was a marked change in the criminal regulatory scheme. Congress had always acted to prevent harm to real children. In the new law, Congress shifted the paradigm from the illegality of child pornography that involved the use of real children in its creation to forbid a "visual depiction" that "is, or appears to be, of a minor engaging in sexually explicit conduct." See 18 U.S.Code section 2256(8)(B).

[77] See Free Speech Coalition v. Reno, 198 F.3d 1083, 1092 (9th Cir. 1999), certiorari granted, 121 S.Ct. 826 (January 22, 2001):

The language of the statute questioned here can criminalize the use of fictional images that involve no human being, whether that fictional person is over the statutory age and looks younger, or indeed, a fictional person under the prohibited age. Images that are, or can be, entirely the product of the mind are criminalized. The CPPA's definition of child pornography extends to drawings or images that `appear' to be minors or visual depictions that `convey' the impression that

a minor is engaging in sexually explicit conduct, whether an actual minor is involved or not. The constitutionality of this definition is not supported by existing case law.

[78] See, e.g., U.S. v. Mento, 231 F.3d 912 (4th Cir. 2000); U.S. v. Acheson, 195 F.3d 645 (11th Cir. 1999).

[79] For more about imposing criminal liability on someone for disseminating information that is publicly available, see section III(D), below.

[80] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, California Criminal Law Review (2001), http://boalt.org/CCLR/.

[81] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, California Criminal Law Review (2001), http://boalt.org/CCLR/.

[82] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, California Criminal Law Review (2001), http://boalt.org/CCLR/.

[83] See, e.g., Fiji Islands, Penal Code, Chapter XXVII ("Larceny, Embezzlement and Conversion") & Chapter XXX ("Robbery and Extortion"). See also Wayne R. LaFave, Criminal Law sectionsection 8.1-8.13 (2000).

[84] See, e.g., Shari'ah Penal Code Law - Zamfara State of Nigeria, Chapter VIII - section 144, http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeChap3-9.html.

[85] See, e.g., German Law Archive, German Penal Code sectionsection 249-252, http://www.iuscomp.org/gla/.

[86] See, e.g., German Law Archive, German Penal Code section 263, http://www.iuscomp.org/gla/; Spanish Penal Code section Article 248 (1), http://www.mcconnellinternational.com/services/country/spain.pdf.

[87] See, e.g., German Law Archive, German Penal Code section 253, http://www.iuscomp.org/gla/.

[88] See, e.g., German Law Archive, German Penal Code section 244, http://www.iuscomp.org/gla/; Revised Penal Code of the Philippines, Book Two, Title Ten, Chapter One, http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm; Shari'ah Penal Code Law - Zamfara State of Nigeria, Chapter VIII - sectionsection 184-193, http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeChap3-9.html.

[89] See, e.g., Swedish Penal Code, Part 2 - Chapter 10 section 1, http://wings.buffalo.edu/law/bclc/sweden.pdf.

[90] See, e.g., Cyber-Extortion Results in Prison Sentence, Net4TV (October 8, 2000), http://net4tv.com/voice/story.cfm?storyid=2931.

[91] See, e.g., Computer Related Embezzlement, New Technologies, Inc., http://www.4incidentresponse.com/cons7.html.

[92] See, e.g., U.S. Securities and Exchange Commission, Internet Fraud: How to Avoid Investment Scams, http://www.sec.gov/investor/pubs/cyberfraud.htm. Compare German Law Archive, German Penal Code section 263, http://www.iuscomp.org/gla/ (fraud) with German Law Archive, German Penal Code section 263a, http://www.iuscomp.org/gla/ (computer fraud).

[93] See, e.g., Security on Trial in Citibank Cyber-Theft Case, The Guardian Newswire (Vol. II, Issue 5), http://www.dlxguard.com/oct97news.htm.

[94] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[95] See, e.g., Security on Trial in Citibank Cyber-Theft Case, The Guardian Newswire (Vol. II, Issue 5), http://www.dlxguard.com/oct97news.htm.

[96] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[97] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[98] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[99] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[100] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[101] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[102] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[103] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[104] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[105] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/. See also Turkey Criminal Code Article 525/a,
http://www.mcconnellinternational.com/services/country/turkey.pdf.

[106] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[107] Cf. 1999 Revision of the Model State Computer Crimes Code, section 6.01.1 and Commentary, http://www.cybercrimes.net/99MSCCC/MSCCC/Article6/6.01.1.html.

[108] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/. This definition of hacking does not, of course, include the further step of gaining access with the purpose of committing further crimes once inside the system; this type of aggravated hacking can be analogized to burglary. See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[109] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California

Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[110] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[111] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[112] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[113] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[114] See, e.g., Brendan I. Koerner, To Heck with Hacktivism, Salon.com (July 20, 2000), http://www.salon.com/tech/feature/2000/07/20/hacktivism/. See also Rachel Munro, May Day Alert: Real or Hype?, ZDNet News (April 30, 2001), http://www.zdnet.com/zdnn/stories/news/0,4586,2713746,00.html?chkpt=zdnn_rt_late st.

[115] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[116] See, e.g., Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[117] See, e.g., Brendan I. Koerner, To Heck with Hacktivism, Salon.com (July 20, 2000), http://www.salon.com/tech/feature/2000/07/20/hacktivism/. The German Penal Code provides an example of how distinct penal laws can address "real world" and "virtual world" damage to property: Section 303 ("Damaging Property") makes it an offense, punishable by a fine or by imprisonment for "not more than two years" , to unlawfully damage or destroy the property of another. German Law Archive, German Penal Code section 303, http://www.iuscomp.org/gla/. Section 304 ("Alteration of Data") makes it an offense, also punishable by a fine or by imprisonment for not more than two years, to unlawfully delete, suppress, render unusable or alter data. German Law Archive, German Penal Code section 304, http://www.iuscomp.org/gla/. Section 303b ("Computer Sabotage") makes it an offense, punishable by a fine or by imprisonment for not more than five years, to interfere "with data processing which is of substantial significance to the business or enterprise of another or a public authority" by violating section 303 or by destroying or damaging a "data processing system or a data carrier". German Law Archive, German Penal Code section 303b, http://www.iuscomp.org/gla/.

[118] See, e.g., Glenn A. Gilmour, Hate-Motivated Violence section 5.0, Department of Justice - Canada, http://canada.justice.gc.ca/en/dept/pub/hmv/ (surveying hate crime laws of various countries). See also What are Hate Crimes?, Stop the Hate, http://www.stopthehate.org/hate_crimes.html (definition of hate crimes).

[119] See, e.g., Jolo, Denial of Service or "Nuke" Attacks (February 21, 2001), http://www.irchelp.org/irchelp/nuke/#netattack.

[120] See, e.g., James Brooke, Teenager Pleads Guilty to Hacking, N.Y. Times (January 19, 2001), http://www.nytimes.com/2001/01/19/technology/19CANA.html (teen-aged hacker pled guilty to denial of service attacks conducted in Feburary, 2000 against various sites, including amazon.com, cnn.com, ebay.com and yahoo.com; the Federal Bureau of Investigation estimated that the attacks caused $1.7 billion in damage).

[121] See, e.g., Alabama Code section 13A-8-10(a)(1) ("A person commits the crime of theft of

services if . . . [h]e intentionally obtains services known by him to be available only for compensation by deception, threat, false token or other means to avoid payment for the services").

[122] See, e.g., Best Online Casinos, http://bestonlinecasinos.com/ (listing online casinos); Jeff Goodell, How to Run a Successful Silicon Valley Business, N.Y. Times (April 8, 2001), http://www.nytimes.com/2001/04/08/magazine/08SILICON.html (prostitutes using web sites to market their services and arrange meetings with customers); SexAddicted: The Best Pornography on the Web, http://www.sexaddicted.com/index.html?bp=google-bottom&bc=pornography.

[123] See, e.g., 1999 Revision of the Model State Computer Crimes Code section 3.02 (using the Internet to disseminate pornography); section 3.03 (using the Internet to promote prostitution), section 7.01 (Internet gambling), section 7.02 (using the Internet to provide alcohol or cigarettes to minors), http://www.cybercrimes.net/99MSCCC/99MSCCCMain.html.

[124] See, e.g., German Law Archive, German Penal Code section 285, http://www.iuscomp.org/gla/ ("Whoever participates in a public game of chance . . . shall be punished with imprisonment"). See also German Law Archive, German Penal Code section 284, http://www.iuscomp.org/gla/ (outlawing unauthorized games of chance). If a jurisdiction lacks laws against gambling or feels they are not adequate to reach online gambling, it can, of course, adopt a cybercrimespecific gambling prohibition. See, e.g., 1998 Model State Computer Crimes Code section 7.01.3, http://www.cybercrimes.net/98MSCCC/Article7/section7013.html.

[125] This argument is especially likely to be made by the operator of an online casino whose web site is maintained in Country A, where the casino is legal, but who is charged with operating a gambling business in violation of local law in Country B. See, e.g., 1998 Model State Computer Crimes Code, Commentary to section 7.01, http://www.cybercrimes.net/98MSCCC/Article7/commentarysection701.html. One way for Country B to avoid dealing with this admittedly difficult issue is to focus its prosecutorial efforts on those who patronize online casinos. See, e.g., 1998 Model State Computer Crimes Code section 7.01.3, http://www.cybercrimes.net/98MSCCC/Article7/section7013.html.

[126] See, e.g., 1998 Model State Computer Crimes Code, Commentary to section 3.03, http://www.cybercrimes.net/98MSCCC/Article3/commentarysection303.html. See also 1998 Model State Computer Crimes Code section 3.03.4, http://www.cybercrimes.net/98MSCCC/Article3/section3034.html (using the Internet to promote prostitution).

[127] See, e.g., 1998 Model State Computer Crimes Code sectionsection 7.02 & 7.03, http://www.cybercrimes.net/98MSCCC/MSCCCMain.html (using the Internet to supply liquor or drugs to minors; using the Internet to sell prescription drugs).

[128] See, e.g., United States of America v. Carl. E. Johnson (No. CR98-5393JRB), Government's Trial Memorandum, http://www.ccc.de/mirrors/jya.com/cej-usbrief.htm ("The defendant was charged . . . with . . . threatening federal judges and officers via the Internet in retaliation for the performance of their official duties").

[129] See, e.g., 1999 Revision of the Model State Computer Crimes Code sectionsection 8.03 & 8.04, http://www.cybercrimes.net/99MSCCC/99MSCCCMain.html. See also Markus Hubner, The Mitnick Story, http://bau2.uibk.ac.at/matic/mitnick.htm:

[A]t age 25, Mitnick was sentenced to one year in a minimum security facility by judge Mariana R. Pfaelzer of the U. S. District Court in Los Angeles Ca. . . .

One year later, Mitnick was released from the facility and assigned a probation officer. Reportably, strange things began to happen. The probation officer's phone was suddenly

disconnected, and the phone company having no record of it. A judge's credit record at TRW inc. was unexplainably altered. Records of Mitnick's arrest and conviction could not be found on the Court's computers at Santa Cruz Ca.

[130] See, e.g., 1999 Revision of the Model State Computer Crimes Code section 8.04.2, http://www.cybercrimes.net/99MSCCC/99MSCCCMain.html.

[131] See, e.g., 17-A Maine Criminal Code sectionsection 454, 456-457, http://janus.state.me.us/legis/statutes/17-A/title17-Ach190sec0.html.

[132] See, e.g., 18 U.S. Code section 115(a)(1)(B) (offense to threaten "to assault, kidnap, or murder, a United States official, a United States judge, a Federal law enforcement officer, or an official whose killing would be a crime under" 18 U.S. Code section 1114. Since this statute focuses on the harm-e.g., the threat-and not on the method used to transmit the threat, it can be applied to online threats as well as to those communicated in person. See, e.g., United States of America v. Carl. E. Johnson, Superseding Indictment - Count Two(No. CR98- 5393JRB), Government,
http://www.ccc.de/mirrors/jya.com/cej040399.htm#Superseding:

On or about June 23, 1997, CARL EDWARD JOHNSON did threaten to murder and aid and abet in the murder of J. Kelley Arnold, a United States Magistrate Judge, with intent to retaliate against Judge Arnold on account of the performance of his official duties, which threat CARL EDWARD JOHNSON transmitted over the Internet, and was received over the Internet at Tacoma, within the Western District of Washington, and elsewhere.

All in violation of Title 18, United States Code, Section ll5(a)(1)(B) and (b)(4) and Section 2.

[133] See, e.g., Arizona Revised Statutes section 13-2809(A):

A person commits tampering with physical evidence if, with intent that it be used, introduced, rejected or unavailable in an official proceeding which is then pending or which such person knows is about to be instituted, such person:

> Destroys, mutilates, alters, conceals or removes physical evidence with the intent to impair its verity or availability; or Knowingly makes, produces or offers any false physical evidence; or Prevents the production of physical evidence by an act of force, intimidation or deception against any person.

See also Georgia Code section 16-10-94(a) ("A person commits the offense of tampering with evidence when, with the intent to prevent the apprehension or cause the wrongful apprehension of any person or to obstruct the prosecution or defense of any person, he knowingly destroys, alters, conceals, or disguises physical evidence or makes, devises,
prepares, or plants false evidence"); Shari'ah Penal Code Law - Zamfara State of Nigeria, Chapter VII - section 326,
http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeChap3-9.html ("Whoever . . . makes any false entry in any book or record or makes any document containing a false statement intending that such circumstance, false entry or false statement may appear in evidence or be used in a judicial proceeding or in a proceeding taken by law before a public servant as such or before an arbitrator and that such circumstance, false entry or false statement so appearing in evidence or so used may cause any person, who in such proceeding is to form an opinion upon the circumstance, entry or statement to entertain an erroneous opinion touching any point material to the result of such proceeding, is said to fabricate false evidence").

[134] See, e.g., Fiji Islands Penal Code section 130, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html:
Any person who, knowing that any book, document or thing of any kind whatsoever is or may be

required in evidence in a judicial proceeding, wilfully removes or destroys it or renders it illegible or indecipherable or incapable of identification, with intent thereby to prevent it from being used in evidence, is guilty of a misdemeanour.

[135] For a sample statute that specifically addresses this type of conduct, see 1999 Revision of the Model State Computer Crimes Code section 8.04.3, http://www.cybercrimes.net/99MSCCC/MSCCC/Article8/8.04.3.html.

[136] See, e.g., 1999 Revision of the Model State Computer Crimes Code, Commentary to section 8.08, http://www.cybercrimes.net/99MSCCC/MSCCC/Article8/8.08.html.

[137] See, e.g., Matt Carolan, The Scandals of Net Vigilantism, ZDNet UK (February 8, 2001), http://www.anchordesk.co.uk/anchordesk/commentary/columns/0,2415,7108262,00.htm; Jason Meserve, Fighting Fire with Fire, Network World Fusion (May 29, 2000), http://napps.nwfusion.com/newsletters/bug/0529bug1.html; Shelley M. Liberto, Vigilantism on the Internet: The "Web Posse" Crosses the Line, http://www.libertolaw.com/4-98.html. See also1999 Revision of the Model State Computer Crimes Code, Commentary to section 8.08, http://www.cybercrimes.net/99MSCCC/MSCCC/Article8/8.08.html.

[138] See, e.g.,1999 Revision of the Model State Computer Crimes Code, section 8.08, http://www.cybercrimes.net/99MSCCC/MSCCC/Article8/8.08.html.

[139] See, e.g., 18 U.S. Code section 115(a)(1)(B) (offense to threaten "to assault, kidnap, or murder, a United States official, a United States judge, a Federal law enforcement officer, or an official whose killing would be a crime under" 18 U.S. Code section 1114.

[140] See http://www.justicefiles.org/.

[141] See, e.g., Michael Ko, Kirkland Sues Over Web Site Listing Officers' Personal Details, Seattle Times (April 3, 2001), http://archives.seattletimes.nwsource.com/cgibin/texis/web/vortex/display?slug=website03m&date=20010403&query=kirkland+police +web+site: [T]he city of Kirkland has filed a lawsuit against the creators of a Web site that lists the home addresses, phone numbers, salaries and, in some cases, Social Security numbers of police officers in that city. . . .Kirkland wants the Web site shut down because of safety concerns, said City Manager David Ramsay. The release of home addresses and Social Security numbers is like `shouting fire in a crowded theater.' . . . A police officer's job, by nature, breeds enemies, and the Web site could be a resource for people seeking retribution, either physically or financially, he said.

[142] See, e.g., 1999 Revision of the Model State Computer Crimes Code section 8.06.1, http://www.cybercrimes.net/99MSCCC/MSCCC/Article8/8.06.1.html:

(A) A person commits the offense of posting confidential information of law enforcement officials when;
(1) they purposefully or knowingly;
(2) cause confidential information;
(3) of a law enforcement official;
(4) to be disseminated via a computer, computer system, computer network, the Internet, e-mail or any other online communication system. (B) Definitions:
(1) confidential information for the purposes of this section is defined as information that is normally not available to the public (i.e. bank account number) or information that a person has taken steps to ensure is not readily available to the public (i.e. unlisted phone number or address).
(2) law enforcement official is defined in Section 8.02(B)(9). (C) Any person who commits this offense is guilty of a fifth degree felony as set out under Section 1.05 of the Model Code.

[143] See, e.g., Netscape White Pages, http://hoe.netscape.com/netcenter/whitepages.html. See also Netscape Yellow Pages,

http://yp.netscape.com/.

[144] See, e.g., Fiji Penal Code sectionsection 50-53, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html. See also Criminal Law of the People's Republic of China, sections 102-112, http://www.qis.net/chinalaw/prclaw60.htm#ChapterI2; Revised Penal Code of the Philippines, Art. 114, http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm/; Swedish Penal Code, Part 2 - Chapter 22, http://wings.buffalo.edu/law/bclc/sweden.pdf.

[145] See, e.g., Fiji Penal Code sectionsection 62-66, sectionsection 79-94, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html. See also Criminal Law of the People's Republic of China, sectionsection 114-138, http://www.qis.net/chinalaw/prclaw60.htm; Swedish Penal Code, Part 2 - Chapter 16, http://wings.buffalo.edu/law/bclc/sweden.pdf

[146] See, e.g., Criminal Law of the People's Republic of China, sectionsection 114-138, http://www.qis.net/chinalaw/prclaw60.htm I2.

[147] See also Criminal Law of the People's Republic of China, sectionsection 140-150, sectionsection 170-190, http://www.qis.net/chinalaw/prclaw60.htm I2.

[148] See, e.g., Samoa Crimes Ordinance, section 42, http://www.vanuatu.usp.ac.fj/Paclawmat/Samoa_legislation/Samoa_Crimes.html; Shari'ah Penal Code Law - Zamfara State of Nigeria, Chapter VII - sectionsection 400-403, http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeChap3-9.html; Swedish Penal Code, Part 2 - Chapter 22 section 1, http://wings.buffalo.edu/law/bclc/sweden.pdf.

[149] See, e.g., Criminal Law of the People's Republic of China, section 102, http://www.qis.net/chinalaw/prclaw60.htm I2; Revised Penal Code of the Philippines, Art. 114, http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm/. See also Fiji Penal Code section 50, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html.

[150] See, e.g., Criminal Law of the People's Republic of China, section 111, http://www.qis.net/chinalaw/prclaw60.htm Chapter I2.

[151] See, e.g., Center for Strategic & International Studies, Cybercrime . . . Cyberterrorism . . . Cyberwarfare, http://www.csis.org/pubs/cyberfor.html:

Using the tools of information warfare, cyberterrorists can overload telephone lines with special software; disrupt the operations of air traffic control as well as shipping and railroad computers; scramble the software used by major financial institutions, hospitals and other emergency services; alter by remote control the formulas for medication at pharmaceutical plants; change the pressure in gas pipelines to cause a valve failure; sabotage the New York Stock Exchange.

[152] See, e.g., Center for Strategic & International Studies, Cybercrime . . . Cyberterrorism . . . Cyberwarfare, http://www.csis.org/pubs/cyberfor.html: The new pervasive tools of information technology blend truth and fiction in ways not easily discernible to decisionmakers. The Internet is also a global superhighway for disinformation. Thus, potentially damaging decisions can be taken as shortened time lines mandate immediate action.

[153] See, e.g., Center for Strategic & International Studies, Cybercrime . . . Cyberterrorism . . . Cyberwarfare, http://www.csis.org/pubs/cyberfor.html.

[154] See, e.g., Danish Criminal Code section 193(1),

http://www.mcconnellinternational.com/services/country/denmark.pdf: Any person who, in an unlawful manner, causes major disturbances in the operation of public means of communication, of the public mail service, of publicly used telegraph or telephone services, of radio and television installations, of data processing systems or of installations for the public supply of water, gas, electricity or heating shall be liable to simple detention or to imprisonment for any term not exceeding four years or, in mitigating circumstances, to a fine.

Cf. 1999 Revision of the Model State Computer Crimes Code section 8.07, http://www.cybercrimes.net/99MSCCC/MSCCC/Article8/8.07.html (sample statute specifically prohibiting the use of computer technology to engage in terroristic acts, including attacks on computer networks, stealing information needed to create weapons of mass destruction, transmitting harmful programs designed to interfere with the operation of computer systems and/or public utilities, etc.).

[155] See, e.g., Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism ("Why a Multilateral Convention"). Commentary on the Draft Convention section 2, http://www.oas.org/juridico/english/monograph.htm.

[156] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 217 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[157] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 217 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[158] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 217 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[159] See, e.g., 1999 Revision of the Model State Computer Crimes Code section 1.03, http://www.cybercrimes.net/99MSCCC/MSCCC/Article1/1.03.html: (A) It is the policy of this state to exercise its jurisdiction over crime and persons charged with the commission of crime to the fullest extent allowable. . . .
(B) In accord with this policy, a person shall be subject to prosecution in this State for an offense he/she commits while he/she is physically located either within or outside this State, by his/her own conduct and/or that of another for which he/she is legally accountable, if:

(1) the offense is committed either wholly or partly within this State; or

(2) the offender's conduct committed wholly outside this State constitutes an attempt to commit an offense within this State; or

(3) the offender's conduct committed wholly outside this State constitutes a conspiracy to commit an offense within this State, and an act in furtherance of the conspiracy was committed within this State, either directly by the offender or at his instigation; or

(4) the offender's conduct committed wholly or partly within this State constitutes an attempt, solicitation, and/or conspiracy to commit in another jurisdiction an offense under the laws of both this State and such other jurisdiction.

(C) An offense is committed partly within this State if either an act constituting an element of the offense, or the result that is an element of the offense, occurs in this State.

(D) When an offense is committed under the laws of this State and it appears beyond a reasonable doubt that the offense or any element thereof took place either in this State or in another jurisdiction or jurisdictions, but it cannot reasonably be determined in which it took place, such offense or element is presumed to have taken place in this State for purposes of this section.

(E) This State's jurisdictional territory includes the land and water within its boundaries and the air space above such land and water within which it either has exclusive or concurrent legislative

jurisdiction. It also includes any computer signals and/or messages received in and/or transmitted from this State. See also 1999 Revision of the Model State Computer Crimes Code, Commentary to section 1.03, http://www.cybercrimes.net/99MSCCC/MSCCC/Article1/1.03.html.

[160] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 217 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[161] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 217 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[162] See, e.g., Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism ("Why a Multilateral Convention"). Commentary on the Draft Convention section 2, http://www.oas.org/juridico/english/monograph.htm: Transnational fraud, for example, has led to decisions by national courts assuming jurisdiction on the basis of any significant connection to the conduct involved. Among these are the States where a fraud was planned, where an effort to defraud was initiated, where individuals worked at implementing the fraud, where or through which communications were made that were intrinsic to the fraud, where the victims were located, and where the fraud had material and intended effects. The widespread recognition of fraud as criminal activity leads States readily to find jurisdiction over such activity, despite the significant relationship particular frauds may have to other States. They tend to assume that punishing fraud will be supported by other affected States, rather than opposed as violating their sovereignty. At the very least, leaving aside the heightened dangers posed by cybercrime, the same rationale that supports such a broad assertion of jurisdiction over fraud supports a similar assertion of jurisdiction over cybercrime.

[163] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 220 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[164] See, e.g., U.S. Code, Federal Rules of Criminal Procedure for the U.S. District Courts, Rule 41(b) ("A warrant may be issued under this rule to search for and seize any (1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense; or (4) person for whose arrest there is probable cause, or who is unlawfully restrained").

[165] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 171 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm: [T[here are some differences with respect to the search of computer data, which may necessitate different or special procedural provisions to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of tangible data. First, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer printout) or intangible form on a physical medium (e.g., diskette), and the tangible medium containing the copy is seized and taken away. In the latter two situations where copies of the data are made, the original data remains in the computer system or storage device. Some changes may be required to domestic law to ensure that intangible data can be searched and seized. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.

[166] See, e.g., Model Code of Cybercrime Investigative Procedure,

http://www.cybercrimes.net/MCCIP/MCCIP.html.

[167] Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ 22 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[168] See Council of Europe, Draft Convention on Cyber-Crime (Draft No. 25 Rev. 5), Chapter II - section 1, - http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm.

[169] See Council of Europe, Draft Convention on Cyber-Crime (Draft No. 25 Rev. 5), Chapter II - section 2, - http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm.

[170] See Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism, http://www.oas.org/juridico/english/monograph.htm.

[171] See Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism, Article 3, http://www.oas.org/juridico/english/monograph.htm.

[172] See Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism, Articles 4-6, http://www.oas.org/juridico/english/monograph.htm.

[173] See Center for International Security and Cooperation, A Proposal for an International Convention on Cyber Crime and Terrorism, Commentary on the Draft Convention section 1, http://www.oas.org/juridico/english/monograph.htm; Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ ¦ 22-30 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm.

[174] See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¦ ¦ 25 (February 14, 2001), http://conventions.coe.int/treaty/EN/cadreprojets.htm ("Although the substantive law provisions relate to offences using information technology, the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved").

[175] For an example of parallel provisions, one addressing conventional criminality and the other addressing cyber-criminality, see, e.g., German Law Archive, German Penal Code section 263(1), http://www.iuscomp.org/gla/ ("Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake, by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine") and German Law Archive, German Penal Code section 263a(1), http://www.iuscomp.org/gla/ ("Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the order of events, shall be punished with imprisonment for not more than five years or a fine").

[176] See Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[177] Donn B. Parker, Is Computer Crime Real?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[178] See Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[179] See Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[180] See Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

[181] See Susan W. Brenner, Is There Such a Thing as Virtual Crime?, ___ California Criminal Law Review ____ (2001), http://boalt.org/CCLR/.

Source: http://www.murdoch.edu.au/ 06/2001