Defining the Boundaries of Computer Crime:

Piracy, Break-Ins, and Sabotage in Cyberspace

Herman T. Tavani
Philosophy Department, Rivier College
htavani@rivier.edu

Recent criminal, or at least questionable, activities involving the use of computer technology[1] have received considerable media attention. Reports of these activities have recently appeared as cover stories in reputable periodicals, as headlines in major newspapers, and as lead stories on television news programs in the U.S. and around the globe. Consider four recent incidents, each of which illustrates a different type of alleged criminal activity involving computer technology. In May 2000, the ILOVEYOU computer virus, also referred to as the *Love Bug*, infected computer systems in the U.S., Europe, and Asia, disrupting e-commerce activities as well as the operations of many governmental agencies. In February 2000, a series of "cyber-attacks" on major commercial Web sites, owned and operated by Amazon, eBay, CNN, Yahoo, and others, resulted in "denial of service" requests to users who wished to access those sites for legitimate purposes. In December 1999, the owners and operators of the Napster Web site were sued by the Recording Industry Association of America for "illegally" distributing copyrighted music (in the form of MP3 files) on the Internet. And in 1998, several dozen computer systems in U.S. military installations and government agencies were successfully broken into, which resulted in a response by the U.S. Defense Department known as Operation Solar Sunrise (see Ghosh and Voas, 1999).[2]

Each of the incidents described in the preceding paragraph would seem to be a genuine instance of computer crime or cybercrime. Other recently reported criminal activities which also involve the use of computer technology, and which might initially appear to be instances of computer crime, arguably are not. For example, there have been reports about pedophiles using the Internet to lure unsuspecting young boys. There has also been at least one reported case of "cyber-stalking" in which a person used a computer to stalk his ex-lover, whom he eventually murdered. We have also heard about incidents in which drug dealers engage in the trafficking of narcotics on the Internet. And there have been reports of individuals using the Internet to distribute child pornography. Should these four examples of criminal activities also be viewed as instances of computer crime? Or are these cases different, in certain important respects, from the four examples that we considered in the preceding paragraph?

In this essay, an attempt is made to establish precise and coherent criteria for determining which criminal activities involving the use of computer technology should count as legitimate instances of computer crime. First, we consider whether having a distinct category of crime called "computer crime" is either necessary or useful. After defending the view that having such a category is indeed worthwhile, at least as a descriptive or informational category of crime, a definition of computer crime is then proposed. Finally, we apply our definition to various criminal activities involving computer technology in order to determine which types of those activities fit and which do not fit the criteria for our proposed definition of computer crime.

Do We Need a Category of Computer Crime?

Before attempting to answer the question whether having a distinct category of computer crime is necessary or even useful, it is important to consider briefly some background issues and discussions involving crime and computer technology that can inform the current debate. For while the recent flurry of criminal activities involving computer technology has been the subject of much media attention, the association of certain kinds of crimes with computers is hardly new. In the 1970s and 1980s, for example, we read about disgruntled employees who altered files in computer databases or who sabotaged computer systems in the act of seeking revenge against employers. Other highly publicized news stories described computer hackers breaking into computer systems—especially those systems thought to be highly secure—either as a prank or as a malicious attempt to subvert data or disrupt its flow. There were also reports, frequently sensationalized and occasionally glamorized by some members of the press, involving hackers who used computers to transfer monetary funds from wealthy individuals and corporations to poorer individuals and organizations. Some earlier reports in the popular media went so far as to portray young computer hackers as "counterculture heroes," single-handedly taking on the "establishment"—i.e., David taking down Goliath (e.g., big government or big business) or Robin Hood raiding the rich and redistributing goods to the poor.[3] Today, however, the attitude of many of those in the media—which itself has been a victim of recent cyber-attacks (e.g., attacks on the New York Times and the CNN Web

sites) — as well as the sentiment of the public in general has shifted considerably. Fewer and fewer individuals and organizations are now sympathetic to the causes of computer hackers, perhaps because of our increased dependence on the Internet. There is a growing concern among those in both the private and public sectors that cyberspace must become a more secure[4] place and that hacking of any type should not be tolerated.

Even though concerns about crimes involving the use of computer technology have received considerable attention in the popular press as well as in certain scholarly publications, the criteria used by journalists and news reporters, as well as by computer ethicists and legal analysts, for determining what exactly constitutes a computer crime has been neither clear nor consistent. For example, there has been some disagreement as to whether crimes involving the presence of one or more computers should necessarily be classified as computer crimes. On the one hand, some news reporters and journalists have seemed, at times, to suggest that any crime involving the presence of a computer is *ipso facto* a computer crime. On the other hand, there are those who have argued that there is nothing special about crimes that involve computers. Gotterbarn (1990), who has criticized much of the earlier media hype surrounding computer-related crimes, could be interpreted as supporting the view that crimes involving computers are not necessarily in need of a special category. He asks, for example, whether we would consider a crime in which an individual uses a surgeon's scalpel in committing a murder to be an issue in medical ethics, simply because a medical instrument was used in the criminal act.[5] And Johnson (1985), in her early writing in computer ethics, defended the view that crime is crime—whether it is committed with or without the use of a computer—suggesting that crimes involving computers are not qualitatively different from crimes in which no computer is present (compare Johnson, 1994).[6]

Based on concerns raised by Gotterbarn and other critics, we can reasonably ask whether having a separate category of computer crime is necessary or even useful. It is perhaps also worth noting that some critics have pointed out that crimes of diverse types are committed in many different sectors, but we don't have separate categories for crimes committed in each of those areas. So it would certainly seem reasonable for these critics to ask why we need a separate category of crime for criminal acts involving computer technology.

To support the position of those critical of the need for a separate category of computer crime, consider three hypothetical scenarios, each of which illustrates a criminal activity involving a computer lab but none of which convincingly demonstrates the need for a distinct category of computer crime. Scenario one: an individual steals a computer device (e.g., a printer). Scenario 2: An individual breaks into the computer lab and then snoops around. Scenario 3: an individual enters a lab that he or she is authorized to use and then places an explosive device, which is set to detonate a short time later, on a computer mainframe or server. Clearly, each of the above acts would be considered criminal in nature. But should any of these criminal acts necessarily be viewed as a computer crime? On the one hand, it would not have been possible to commit any of these three crimes in precisely the same manner if computer technology had never existed. This factor might initially influence some to believe that these three criminal acts are somehow unique, or somehow special, to computer technology. Yet the three criminal acts in question can easily be understood and prosecuted as specific examples of ordinary crimes involving theft, breaking and entering, and vandalism, even though each criminal act coincidentally happens to involve the presence of computer technology.

Considering our analysis thus far, one might be inclined to infer that there are no legitimate grounds for having a separate category of computer crime. But would such an inference be justified at this point? Putting aside that question for the moment, one still might ask what practical purpose would be served in our framing such a category of crime. For example, would having a category of computer crime help us to understand better certain nuances of illegal or immoral activities involving computer technology? Or might having such a category of crime be helpful in prosecuting certain criminal activities involving the use of this technology that otherwise would be more difficult to prosecute under conventional legal statutes? Let us briefly consider some possible reasons for framing one or more categories of computer crime.

Legal, Moral, and Informational/Descriptive Categories of Computer Crime

Arguments for having a category of computer crime can be advanced from at least three different perspectives: legal, moral, and informational or descriptive. We consider arguments for each, beginning with a look at computer crime as a separate *legal* category. From a legal perspective, computer crime might be viewed as a useful category for prosecuting certain kinds of crimes. For example, in some states in the U.S. crimes involving handguns can be prosecuted under the legal category of handgun crime. That is, in certain states criminal legislation has been proposed and enacted into law, based on the notion that crimes involving handguns are worth distinguishing, for relevant purposes, from similar crimes in which no handguns are present. So even though a critic like Gotterbarn is correct in pointing out that a murder committed with a surgeon's scalpel would not be treated as a separate category of murder, and even though, in one sense, murder is murder whether it involves the use of a scalpel, an ice pick, or a handgun, current criminal laws in certain states nonetheless distinguish between crimes committed with and without the use, or even the presence, of a handgun. Per-

haps, then, the same kind of reasoning could be applied to crimes involving computer technology.

We can, of course, inquire into the value of having a separae legal category of handgun crime and we can ask whether that particular category of crime is always clear in its implementation. For example, if *X* assaults *Y* by striking a blow to *Y's* head with a handgun, should that crime be prosecuted as a handgun crime simply because a handgun is used? Also, if *Z* uses a fake (or toy) handgun to rob a convenience store, should that crime be prosecuted as a handgun crime? In the first scenario, a handgun was used in, but was not essential to carrying out, the crime since many different kinds of devices or objects (e.g., a hammer, a rock, or even a computer hardware device) could have been used by *X* to assault *Y*. And in the second situation, no genuine handgun was used in the crime. However, legislation concerning handgun crime has been written in such a way that, in a criminal act, the mere presence of a handgun or the use of a device that might give the impression of being an authentic handgun is sufficient for that criminal act to be prosecuted as an instance of handgun crime.

How do the two scenarios in the preceding paragraph, both of which involve crimes that can be prosecuted under the category of handgun crime, affect our question of whether crimes involving computer technology should also be treated as a separate legal category of crime? For one thing, both scenarios illustrate some of the problems inherent in attempts to draft clear and coherent legislation involving a special *category* of crime. In deciding whether to frame a distinct category for crimes involving handguns, it might initially seem that drafting appropriate legislation would be a relatively straightforward and unproblematic process. However, we have seen some of the confusions that can result in prosecuting all criminal acts involving the presence of one or more handguns under a general category of crime. This can help us to anticipate some of the challenges we might face in deciding whether to prosecute all crimes involving the use or presence of computer technology under a specific legal category of computer crime.[7]

Independent of arguments for whether it is useful to have a distinct legal category of computer crime, questions can be raised about the usefulness of computer crime a as a *moral* category. Johnson and Nissenbaum (1995) note that because computer crime is a "territory" that is not so well defined, a number of ethical questions both "precede and follow from" declaring certain computer-related activities illegal. They note, for example, that we can still reasonably ask questions such as: Which forms of online behavior should we criminalize? Are current illegal forms of online behavior inherently immoral or are they considered immoral only because they are declared illegal? Are current forms of punishment for online criminal acts fair? An additional problem in determining whether crimes involving computer technology justify the need for a separate moral category is that many of the ethical issues associated with computer crime also border on distinct, but related, issues involving intellectual property, personal privacy, and free speech in cyberspace.

In addition to the legal rationale and the moral rationale, a third rationale for having a category of computer crime is one that can be viewed as *descriptive* or *informational* in nature. That is, one virtue of having a category of computer crime as a purely descriptive rubric is that it could help us gain a certain level of clarity and precision in analyzing crimes involving the use of computer technology. On pragmatic grounds, having such a category might better enable us to determine which characteristics currently used to link together crimes associated with computers are relevant and which are not. In our effort to provide an adequate definition of computer crime, our primary interest in the present study will be with computer crime as a descriptive, rather than as a legal or moral, category of crime.

Computer Crime as a Descriptive Category of Crime

At the outset, one might reasonably ask what the value would be in pursuing questions about computer crime from the point of view of a descriptive category. One argument to support the view that having a descriptive category of computer crime is worthwhile can be advanced by appealing to an insight of James Moor's with respect to certain conceptual confusions that have arisen because of the development and use of computer technology. Moor (1985, 1998) points out that computers create "new possibilities" and new situations which, in turn, give rise to ethical and social issues that are not easily anticipated and that are not always able to be subsumed under existing policies and laws. As a result, we are left with what Moor calls "policy vacuums." Initially, it might seem that we could simply either extend some of our existing policies or frame new policies to fill these vacuums. But this move will not always work, Moor claims, because computer technology also presents us with certain conceptual vacuums or what he calls "conceptual muddles." Consider, for example, the concept of computer software. Before we can determine whether to have a policy that would grant legal protection to software as a form of property, we must first answer the question: "What exactly *is* computer software?"

We can apply Moor's model regarding the process of identifying conceptual vacuums that arise because of the use of computer technology in general to identifying some of the specific confusions that emerge because of criminal activities made possible by computer technology. So in showing why a separate category of computer crime as a descriptive category is justifiable on pragmatic grounds, we can begin by noting that computers make possible certain kinds of crimes that otherwise would not have been possible in the pre-computer era. We can next see why, because of certain conceptual confusions or muddles surrounding computer technology, the exact nature of some of the criminal activi-

ties involving computer technology is not always clearly understood. We can also see, then, why our existing laws and policies can not always be extended to cover adequately at least certain kinds of crimes involving computers. Thus it would seem that having a descriptive category of computer crime might enable us to resolve some of the conceptual confusions and muddles underlying crimes involving computers, which could also eventually help us to frame some coherent normative (legal and ethical) policies regarding computer crime.

Establishing Clear and Coherent Criteria

We next consider which specific criteria would be essential for framing a plausible definition of computer crime. Perhaps a computer crime could, as Forester and Morrison (1994) suggest, be defined as a criminal act in which a computer is used as the "principal tool." On that definition, the theft of a computer hardware device—e.g., the theft of a printer as we considered in an earlier scenario—or, for that matter, the theft of an automobile or a television which also happened to contain a computer component (e.g., a microprocessor), would not count as an instance of computer crime, since a computer is not the principal tool for carrying out the crime. Even though such cases of theft can involve computer technology in some sense—i.e., the presence of one or more computers or computing devices—a computer is not the principal tool used to carry out the criminal act. The same line of reasoning could also be applied to the cases we considered above involving the breaking and entering into the computer lab as well as the vandalizing a computer system in the lab. Forester and Morrison's definition, then, correctly rules out the three examples of crimes involving activities in a computer lab that we considered above.

At first glance, Forester and Morrison's definition of computer crime might seem plausible. But is such a definition satisfactory? Consider the case of someone who uses a personal computer to process his federal income tax returns. Let us call him Bill. In the act of completing his income-tax forms, Bill decides to cheat the government by filling in false information on the forms of his online tax-return program package in his personal computer. In this case, a computer is arguably the principal tool used by Bill to carry out the criminal act. But should this particular criminal act be considered a computer crime? Surely, Bill could have committed the same crime by manually filling out a standard (hardcopy) version of the income-tax forms by using a pencil or pen. That Bill happened to use a computer rather than a pen or pencil in the act of committing the crime is coincident with, but by no means essential to, this particular criminal act. So it would seem that Forester and Morrison's definition of computer crime is not adequate.

Taking into account Moor's point that computer technology creates new possibilities—and by extension, new possibilities for crime—as well as Forester and Morrison's point that computer technology provides a tool that can be used to carry out certain kinds of criminal acts, perhaps we can put forth a definition of computer crime that incorporates both insights. It is argued that for a criminal act to count as a genuine instance of computer crime, the act must be one that *can be carried out only through the use of computer technology*. Limiting genuine computer crimes to ones that can only be carried out "only through the use of computer technology" would incorporate Moor's insight that new opportunities (including new possibilities for crime) are made possible because of the existence of computer technology. And including in our definition the fact that computer technology provides the means for carrying out certain criminal activities also incorporates Forester and Morrison's insight regarding computer technology as a "tool" that can be used in certain crimes, while at the same time restricting the range of crimes that will count as genuine computer crimes. For example, our proposed definition would rule out as a genuine instance of computer crime an act in which an individual uses a computer to cheat on his income tax return. It would also preclude as a genuine computer crime a criminal act in which a computer device was used in the act of assaulting someone. That is, neither the criminal act of cheating on one's income-tax form nor the act of assaulting an individual depends on the existence of computer technology to carry out the particular criminal act.

Applying the Definition to Some Specific Cases

In the introductory section of this essay, we considered four examples of criminal activities involving computers which, intuitively, appeared to be genuine computer crimes and four examples that seemed possibly to border on being genuine computer crimes but were also questionable cases. Because criminal acts such as "attacking" commercial Websites, unleashing of the "love bug" virus, distributing MP3 files on the Napster Web site, and breaking into the U.S. government and military computer systems all satisfy our newly proposed definition of computer crime, we can now see why each of those activities can be classified as genuine instances of computer crime.

We can also see why those borderline or "questionable" cases also considered in the introductory section—viz., criminal activities involving pedophiles, drug traffickers, child pornographers, and (cyber) stalkers using the Internet to commit their criminal acts—are not, strictly speaking, computer crimes. First, consider the specific case involving pedophile activities on the Internet. Admittedly, a criminal act in which a pedophile uses the Internet to lure young boys might initially be thought of as an instance of computer crime. However, pedophiles have engaged in the practice of luring unsuspecting children long before the introduction of computers and the Internet. And although computer technology can be used as a tool—and perhaps even the principal tool—to carry out pedophile-related criminal acts, such crimes can

be (and have been) carried out in ways that do not involve computer technology. Pedophiles can, for example, use telephone directories or lists that contain the names of children attending a certain elementary school or day-care facility to assist them in their criminal activities. So, based on the proposed definition of computer crime put forth in this study, cases involving the use of computer technology by pedophiles to lure children would clearly not count as instances of computer crime.

The same reasoning process used in the pedophile example, of course, would apply to the three other "questionable" examples of criminal acts involving the Internet that were also briefly mentioned in the introductory section of this essay. So we can now see why the examples of trafficking drugs, distributing child pornography, and stalking an ex-lover, each of which also happened to involve the use of computer technology as a tool in carrying out particular criminal acts, are also not genuine instances of computer crimes.

Three Types of Computer Crime: Piracy, Break-ins, and Sabotage in Cyberspace

Which specific types of criminal activities will count as genuine instances of computer crime, and how could we catalogue those crimes? On the criteria suggested above, one type would include the set of activities involving the use of computer technology to make one or more unauthorized copies of (i.e., "pirating") proprietary software. Another type would include the range of activities involving the use of computer technology by one or more individuals to gain unauthorized access to (i.e., break into) another party's computer system, whether for amusement or for personal gain. And a third type would include those activities in which one or more individuals uses computer technology to unleash a software program designed to sabotage a computer system or computer network by disrupting system activities on a privately owned computer system or on the Internet, or by damaging or destroying data or system resources, or both. In each of these three types of criminal acts, the crime can be carried out *only* through the use of computer technology. Crimes that fit our definition would fall into one of three distinct categories:

(1) *Software Piracy*—using computer technology to (a) produce one or more unauthorized copies of proprietary computer software, or (b) distribute unauthorized software or make copies of that software available for distribution over a computer network.

(2) *Electronic Break-Ins*—using computer technology to gain unauthorized access either to an individual's or an organization's computer system, or to a password-protected Web site.

(3) *Computer Sabotage*—using computer technology to unleash one or more programs that (a) disrupt the flow of electronic information across one or more computer networks, including the Internet, or (b) destroy or damage data and computer system resources.

Each of these three categories of computer crime is discussed in greater detail in a longer version of this essay (in Spinello and Tavani, forthcoming). Let us briefly consider how each of the four crimes discussed in the introductory section of this study fit into one of these three categories. Recall the four examples: (i) distributing MP3 files (which include copyrighted material) on the Internet via the Napster Web site, (ii) breaking into to U.S. government and military computer systems, (iii) unleashing the "love bug" computer virus, and (4) "attacking" commercial Web sites so that they would issue "denial of service" requests. On the model of computer crime advanced in this study, each of these recent incidents falls into one or more of the three distinct types of computer crime articulated. For example, the distribution of MP3 files involved in the Napster case falls under the category of software piracy (category 1), while the unleashing of the "love bug" virus clearly falls under computer sabotage (category 3). Unauthorized entries into military and government computer systems are a clear example of electronic break-ins (category 2).

But how should we classify the cyber-attacks directed at the targeted commercial Web sites? That is, how would such a criminal act map into one of our threefold distinctions regarding the categories of computer crime that we have articulated? Because the attacks on these Web sites disrupted activities on the Internet by resulting in "denial of service" requests for users who wish to access those particular sites for legitimate purposes, these recent cyber-attacks would seem to fall into our third category: computer sabotage. However, since these attacks also involved the unauthorized use of (i.e., the breaking into) third party computer systems (in universities and other organizations) to send "spurious requests" to the Web sites in question, these attacks would also fall into our second category of computer crime—viz., computer break-ins. So the recent cyber-attacks on commercial Web sites would seem to span two distinct categories of computer crime.

Concluding Remarks

We began this study by considering whether having a distinct category of computer crime is necessary or even useful. We then noted that arguments for having such a category of crime could be advanced from legal, moral, and descriptive/informational perspectives. Appealing to Moor's insight regarding certain "conceptual muddles" that arise from computer technology, we saw that having a descriptive category of computer crime could help to eliminate some of the conceptual confusions with respect to criminal activities associated with computer technology. We then set out to define the boundaries of computer crime. Showing that Forester and Morrison's definition was inadequate, we argued that for any criminal act to count as an instance of computer

crime, it must be such that it can be carried out *only* through the use of computer technology. In applying that definition, we saw that any genuine instance of a computer crime would typically fall into one of three types: software piracy, electronic break-ins, and computer sabotage.[8]

We have also noted that computer technology, especially the Internet, has provided a new forum for certain illegal activities which, at first glance, might seem like instances of computer crime. On closer inspection, however, some of these criminal acts turned out not to be computer crimes at all—at least not in the strict sense of that that category of criminal activity which we have defended in this essay. We can now see why some of those crimes—e.g., certain crimes involving pedophiles, drug traffickers, child pornographers, and cyber-stalkers that we briefly described in the introductory section of this essay—are not, strictly speaking, computer crimes despite the fact that computer technology was a means used for carrying out those criminal acts.

The threefold division of computer crime advanced in this essay could be challenged by certain recent online incidents,[9] and future cases of criminal activity involving computer technology may cause us to reexamine the tripartite scheme. One recent form of criminal activity that seems potentially to border on computer crime is a criminal act involving the use of digital telephony. Baase (1997) points out that in the use of cellular phones, a popular technique for avoiding charges is "cloning"—i.e., reprogramming one's cellular phone to transmit another customer's name. When true "computer telephony" (the merging of computers and telephones, also known as Internet phones or I-phones) arrives, we may need to reexamine our proposed definition of computer crime and we may discover the need to modify, or possibly even expand on, the three types of activities that we have defended as genuine instances of computer crime. For the time being, however, one virtue of having a working model of computer crime in place is that we can appeal to a consistent set of criteria in determining which new or evolving forms of illegal activities that involve existing computer technology should and should not count as genuine instances of computer crime.

Our primary interest in this essay has been to establish criteria for computer crime as a *descriptive category*. It may well be that for reasons beyond those considered in this study, law makers will decide to frame a definition of computer crime or cybercrime as a legal category that makes any criminal activity on the Internet a form of cybercrime. In the same way that certain law makers and law-enforcement representatives have supported a legal category of handgun crime in which the mere presence of a handgun in a criminal act would be sufficient for that act be prosecuted as a handgun crime, law makers may decide to frame an Internet crime law in such a way that the mere use of the Internet to carry out a criminal act would be sufficient to have that criminal act prosecuted as an instance of Internet crime or cybercrime.[10] However, our purpose in considering computer crime as a descriptive category, rather than as a legal or as a moral category, has been to gain a clearer understanding of those conditions which separate genuine computer crimes from those criminal activities in which computer technology is: (a) merely present in some form, or (b) used in a way simply to assist in carrying out a type of criminal activity that otherwise could have been carried out without the presence or use of computer technology. In this sense, then, having a descriptive category of computer crime can help us eliminate certain confusions currently associated with a range of criminal activities, many of which involve computer technology in ways that such technology either is merely present in the crime or is used as a tool that assists or possibly even enhances certain criminal acts, rather than providing the means essential to carrying out those acts. ◆

References

Baase Sara (1997). *A Gift of Fire: Social, Legal, and Ethical Issues in Computing*, Upper Saddle River, NJ: Prentice Hall.

Branscomb, Anne W. (1990). "Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime," *Rutgers Computer and Technology Law Journal*, Vol. 16, pp. 1-6.

Forester, Tom and Perry Morrison (1994). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. 2nd ed. Cambridge, MA: MIT Press.

Ghosh, Anup K. and Jeffrey M. Voas (1999). "Innoculating Software for Survivability," *Communications of the ACM*, Vol. 42, No. 7, July, pp. 38-44.

Gotterbarn, Don. (1990). "Computer Ethics: Responsibility Regained," *National Forum: The Phi Kappa Phi Journal*. Reprinted in *Computing, Ethics & Social Values*. edited by D. G. Johnson and H. Nissenbaum (1995). Englewood Cliffs, NJ: Prentice Hall, pp. 18-24.

Jajodia, Sushil, Catherine D. McCollum, and Paul Ammann (1999). "Trusted Recovery," *Communications of the ACM*, Vol. 42, No. 7, July, pp. 71-75.

Johnson, Deborah G. (1985). *Computer Ethics*. Englewood Cliffs, NJ: Prentice Hall.

Johnson, Deborah G. (1994). *Computer Ethics*. 2nd ed. Englewood Cliffs, NJ: Prentice Hall.

Johnson, Deborah G. and Helen Nissenbaum, editors (1995). *Computing, Ethics & Social Values*, Englewood Cliffs, NJ: Prentice Hall.

Levy, Steve. (1984). *Hackers: Heroes of the Computer Revolution*. Garden City, NY: Doubleday.

Moor, James H. (1985). "What is Computer Ethics?" *Metaphilosophy*, Vol. 16, October, pp. 266-275.

Moor, James H. (1998). "Reason, Relativity, and Responsibility in Computer Ethics," *Computers and Society*, Vol. 28, No. 1, pp. 14-21.

Spinello, Richard A. and Herman T. Tavani, editors (forthcoming). *Readings in Cyberethics*. Sudbury, MA: Jones and Bartlett Publishers.

Tavani, Herman T. (1999). "Social and Ethical Aspects of Information Technology," *Wiley Encyclopedia of Electrical and Electronics Engineering* (Vol. 19). edited by J. G. Webster. New York: John Wiley and Sons Publishers, pp. 413-425.

Tavani, Herman T. (2000). "Privacy and Security." Chap. 4 in *Internet Ethics*. edited by D. Langford. London, UK: Macmillan Publishers.

Wessells, Michael G. (1990). *Computer, Self, and Society*, Englewood Cliffs, NJ: Prentice Hall.

Acknowledgments.

I am grateful to Lloyd Carr, Chuck Huff, Deborah Johnson, and Jim Moor for their helpful comments on an earlier draft of this essay.

Notes:

1 - By "computer technology" I mean the range of computing technologies that include stand-alone personal computers, privately owned computer systems and networks (e.g., LANs and WANs), and the Intenet itself.

2 - Although reports about unauthorized entries into government and military computer systems have received considerably less media coverage than that given to recent attacks on commercial Web sites, break-ins to government and military systems are arguably more serious because of the threat they pose to national security. In light of recent attacks by hackers on government computer systems, some authors have warned us of the importance of defending against the possibility of "information warfare" (see Jajodia, McCollum, and Ammann, 1999) and cyber-terrorism.

3 - In a separate paper (Tavani, 1999), I describe specific examples of some of these earlier computer crimes. For an in-depth discussion of earlier computer crimes, including the rise of the "hacker culture," see Levy (1984) and Wessells (1990).

4 - Recently, much of the discussion about online activities involving electronic break-in as well as the discussion about sabotage or disruption to computer system resourses (in the form of computer viruses) has been categorized under the label of computer security rather than under the heading of computer crime. Unfortunately, this shift in categorization has lead to certain confusions involving computer security. I have argued elsewhere (Tavani, 2000) that "computer security" is an ambiguous expression and one that is often used equivocally. In one sense, "security" in the context of computer technology has come to be identified with the set of concerns involving a computer system's vulnerability to "attacks" from viruses or worms or what Branscomb (1990) describes more generally as "rogue computer programs." There is another sense of "security," which intersects with issues related to privacy, that is concerned with the protection of personal and proprietary information from unauthorized access—i.e., the protection of information that resides in databases as well as information that is communicated over the Internet (e.g., e-mail). These two senses of "security" are sometimes confused in the current literature on computer security.

5 - It must be noted that Gotterbarn never explicitly asserts that there is no need for a category of computer crime; instead, he argues that crimes involving computers are not necessarily issues in computer ethics. In holding that position, however, he seems to have supported the view that such crimes are not essentially "computer crimes" but are simply instances of ordinary crimes, which also happen to involve the use or presence of one or more computers.

6 - In the second edition of *Computer Ethics* (1994), Johnson modifies her earlier position on computer crime and devotes an entire chapter to that topic.

7 - Perhaps a more practical problem involved in prosecuting computer crimes, at least those involving the Internet as well as some privately owned Wide Area Networks (WANs), has to do with jurisdictional issues. For example, can someone who resides in one state (e.g., New York) and who operates a Web site whose content is perfectly legal in that state, but illegal in certain states where that content can also be viewed online, be prosecuted by law enforcement personnel from the state in which that content is illegal (e.g., Texas)? Not only are there interstate problems associated with prosecuting crimes involving the Internet, but there are also problems of international law to be considered. The Council of Europe is currently considering some of these issues, and on April 27, 2000 it released a first draft of an international convention of "Crime in Cyberspace" (see http://conventions.coe.in/treaty/en/projects/cybercrime.htm). Although issues pertaining to jurisdictional concerns are important for criminal acts involving computer networks, such issues are not considered in the present study.

8 - James Moor has pointed out to me that to limit the number of genuine computer crimes to the three types that I am proposing, an additional qualification is needed. Moor notes that we could imagine a possible case in which a criminal act involving the unauthorized cracking of a safe could be accomplished *only* through the use of a computer. On the definition of computer crime I have proposed, this act would seem to qualify as a genuine instance of computer crime, even though that specific criminal act would not fit into any of the three types of genuine computer crimes described above. Hence, Moor suggests an additional condition—*viz.*, the qualification that the criminal act *can occur only within computer technology*. When this condition is brought into the definition, we see that computer technology is not only the necessary means for committing a genuine computer crime it is also the necessary *location* of the crime. I pursue Moor's important suggestion on this point in a longer version of this essay.

9 - Chuck Huff has pointed out to me an interesting case involving LambdaMOO, which might challenge the tripartite model of computer crime I have proposed. The incident in question is an alleged "virtual rape" that occurred when one MOO player "took over" two players' characters and had them perform various obscene acts in the context of that MOO, which is a "public space." The LambdaMOO incident raises a number of interesting questions. First, we can ask whether this particular form of online behavior constitutes a *criminal* act. Assuming the act is criminal in nature, we can next ask whether the act qualifies as a *computer* crime. (Clearly this particular act could not have been carried out if computer technology did not exist.) We might begin by asking whether the behavior involved constitutes a form of rape under our current legal statutes, and then ask whether the notion of "rape" (as understood in physical space) can be extended to apply to virtual space as well. Although at this point I am not prepared to accept the claim that a genuine computer crime has occurred on LambdaMOO, I recognize that incidents such as this clearly pose a threat to my threefold model.

10 - Also, law makers might wish to frame a cybercrime law in which a subset of crimes assisted by computer technology would also be included. For example, law makers might elect to group certain crimes involving the use of computer technology, such as those involving pedophilia, cyber-stalking, drug trafficking, and child pornography, into crimes that can be prosecuted as cybercrimes. Even though these four crimes, each of which is enhanced by computer technology, do not fit our definition of a pure computer crime, it could be argued that each crime involves the use of computer technology in ways that certain crimes which involve computer technology only incidentally—e.g., crimes involving theft, break-ins, or vandalism in a computer lab—do not. That is, computer technology can assist pedophiles, drug traffickers, pornographers, and stalkers in significant ways that enhance the committing of those crimes, especially in terms of both ease and scale. However, in the case of other crimes that happen to involve the mere presence of computer technology—e.g., the examples of crime involving the computer lab—the role of computer technology in carrying out the particular