11-13-2012

Cybercrime and the Law: Challenges, Issues, and Outcomes

Susan W. Brenner
University of Dayton, susanwbrenner@yahoo.com

INTRODUCTION: TWENTY-FIRST-CENTURY BONNIE AND CLYDE

The legal, practical, and political issues implicated by cybercrime and other cyberthreats have received a great deal of attention in specialized publications, most of which are directed at corporate or government professionals who work in this area. I continue to be amazed at the extent to which cyberthreats—those that already exist and those that will come into existence in the very near future—are ignored or overlooked by the mainstream media.

Those of us who work in this area know all too well that the number of cyberattacks on government and civilian targets increases in frequency and severity with every passing month. If these attacks took place in the terrestrial world—in real space rather than in the virtual space of the Internet—they would receive a barrage of media attention. Since the attacks play out in cyberspace, they remain invisible unless one knows where and how to find information about them. Finding information about cyberattacks is a challenge, in part because the major players—the corporate and government entities that become the victims of attacks and the cybercriminals and state-sponsored hackers who launch the attacks—generally have no interest in "outing" the incidence and details of an accelerating pattern of cyberconflict.

This is a book for those who would like to learn about cyberconflict—about how the traditional battle between good and evil (or, perhaps more

accurately, between what some perceive as good and evil) is manifesting itself in cyberspace. More precisely, this is a book for those who would like to learn about how the law applies—and in some instances does not apply—to the two dominant types of cyberconflict: cybercrime and cyberwarfare. Each represents the migration of a traditional, real-world threat (crime and war) into cyberspace.

The migration of these threats into cyberspace alters them in ways that make the application of traditional law increasingly problematic. It also erodes the effectiveness of the control mechanisms sovereign entities—nation-states—have historically used to control the incidence and severity of these threats to social order. This, in turn, produces an increasingly untenable situation that is—or should be—of concern to both governments and private citizens. If nation-states cannot respond effectively to cybercrime and cyberwarfare, there is little, if any, disincentive for those who are so inclined to engage in either, or both.

As chapter 8 explains, governments control crime by creating disincentives to break the law; in other words, the likelihood that I will be captured, convicted, and sentenced to prison creates a disincentive that deters me, and others like me, from robbing banks and committing other crimes. The downside of criminal activity outweighs its attractiveness, and a similar set of disincentives usually discourages nation-states from warring with each other. Cyberspace makes it possible for criminals or agents of a nation-state to carry out attacks remotely and anonymously, which erodes the likelihood that those responsible will be identified, captured, convicted, and punished. That, in turn, erodes, if it does not entirely erase, the disincentives for engaging in such conduct; absent such disincentives, activities such as online bank theft become attractive endeavors, at least for some. And that creates the possibility that cybercrime and cyberwarfare will increase in incidence to the point at which they threaten the stability of nation-states, in varying ways and varying degrees.

This is a state of affairs that should be of interest to students and professionals in various fields, such as computer technology, political science, and economics, because they will likely have to deal with the consequences of cyberconflict and the insecurity it generates. These consequences will also be of interest to concerned citizens, who want to understand the national security implications of our increasing use of cyberspace.

The possibility that cyberconflict will become a phenomenon that

threatens the stability of nation-states is of great concern to many governments, including the United States. The United States is perhaps the primary target for cybercriminals and is likely to become a primary target of cyberwarfare.

This book analyzes both cybercrime and cyberwarfare but devotes most of its analysis to cybercrime, for two reasons. One is that governments have been dealing with cybercrime for almost thirty years and therefore know more about the challenges it creates for lawmakers and law enforcers. The other reason is that there are so far no confirmed instances in which one nation-state has launched cyberwar attacks on another; there are instances in which it appears that one state was the victim of attacks launched by a hostile state, but the circumstances involved are too ambiguous to determine the nature of the attack with any degree of confidence, given the requirements of current law.

Approaching Cybercrime and the Law

Cybercrime and the Law deals with the intersection of cyberconflict—that is, cybercrime and cyberwarfare—and the law. Since I am a U.S.-trained lawyer, I know more about U.S. law than I do about the law of other countries; this book will therefore focus primarily on how U.S. law applies, does not apply, and perhaps should apply to various types of cybercrime and to certain manifestations of cyberwarfare. Focusing on U.S. cyberconflict law also has a utilitarian aspect: since the United States has been dealing with cybercrime for well over two decades, and since the United States is a federal system composed of a single federal government and fifty independent state governments, it generates a great deal of law, at both levels. This means that U.S. cybercrime law is diverse, complex, and at least to some extent more sophisticated than the cybercrime and cyberconflict law of other countries.

Since this is a book about cyberconflict law, and since I am a lawyer, this book uses the approach law schools take in training future lawyers and the approach lawyers take when practicing law. That is, it focuses on three dimensions of cyberconflict: the applicable law itself; the policies responsible for that law; and how discrete facts impact the application of the law.

Legal analysis is, as lawyers, law students, and law professors say, "fact sensitive." To illustrate, assume that John Doe, a convicted burglar, is

incarcerated in the Monroe State Prison. Doe has a disease that is inevitably fatal; it will kill him but will take some years to do so. While in prison, Doe becomes angry with William Brown, one of the guards, and, when the opportunity arises, attacks the guard, biting him viciously.[1] Doctors examine Brown and determine that the bite infected him with Doe's fatal illness; Brown will die of the illness but, like Doe, may survive for years before succumbing to it.

The state has a statute that defines murder as "purposely causing the death of another human being." By infecting Brown with the disease, Doe has "caused" him to die of that disease (unless some other factor intervenes before it can kill him). Doe infected Brown purposely; he wanted to kill Brown, so the intent element of the crime is met. The local prosecutor charges Doe with murdering Brown. Doe's lawyer argues that he cannot be charged with murdering Brown because Brown is still alive; the prosecutor argues that, by infecting Brown with the disease, Doe killed him, in effect. Doe's lawyer argues that he cannot be prosecuted for murdering Brown (if at all) until (1) Brown dies and (2) an autopsy establishes that the disease was the sole cause of his death. The prosecutor argues that he can pursue Doe now because he did everything he could to kill Brown and has killed Brown (unless and until some other factor intervenes to cause his death).

This issue has arisen in real cases.[2] It illustrates how complicated it can be to apply even a simple statute, such as a murder statute, to a real-life set of facts. In deciding whether Doe can be prosecuted for Brown's murder (while Brown is still living), the judge who has the case will have to analyze the specific facts at issue, such as the fatality of the disease, the likelihood that a cure will be developed, Brown's possible resistance to it, and so forth, plus the plain language of the law and the policies behind the law. As to the latter, the prosecutor will probably argue that Doe has done everything he can to kill Brown and will kill Brown, absent possible intervening circumstances, and so should be treated as a murderer. The judge will have to sort all of that out and decide what is to be done with Doe while trying to ensure justice for Brown.

Hence, unlike other disciplines in which white is white and black is black or 1 is 1 and 2 is 2, in the law white can be white, black, purpose, or something other than a color, and 1 can be 1, 15, 1,999,444,122, or not even a number. Lawyers analyze and argue, and the law develops and ex-

pands through that process. Because that is the methodology of the law, law schools use casebooks, books that compile relevant, illustrative cases to train future lawyers. Students read cases—like the hypothetical case outlined above—and then analyze the arguments that can be made for both sides and argue about what is the correct outcome.

This book uses statutes and cases to illustrate the various aspects of cyberconflict law, its strengths and limitations, and how it plays out in particular instances. Some of the chapters—such as chapters 1 and 2—explain why cyberconflict, and particularly cybercrime, have required the creation of new law. Many of the activities that fall into the category of cybercrime simply do not fit into traditional law; in effect, they create challenges for existing law that are far, far more complicated than the issues involved in the Doe-Brown hypothetical outlined above. To understand the law as it currently exists, it is necessary to understand why that law was needed and how it was crafted. Understanding both also helps the reader to understand how, and why, many of our cybercrime laws are works in process, that is, might need to be revised as our experience with the dark side of cyberspace increases.

A Note on Cybercrime

Readers of this book may wonder how, if at all, cybercrime differs from crime.[3]

Crime consists of engaging in conduct that has been outlawed by a human social grouping, such as a tribe, city-state, or nation-state, because it threatens the society's ability to maintain social order.[4] Social order cannot exist without rules that proscribe certain harmful types of activity and institutions that enforce these rules. These rules constitute a society's criminal law. Criminal law is designed to prevent the members of a society from preying on each other in ways that undermine social order. It does this by defining certain types of behavior as intolerable, as crimes.

Crimes take many forms because each targets a particular harm. As we all know, there are crimes that encompass harming individuals (murder, rape, and assault), property (arson, theft, and vandalism), government (obstructing justice, treason, and riot), and morality (obscenity and gambling). Since societies have dealt with crime for millennia, they have developed standardized definitions of the core real-world crimes. In

addition to these core crimes, modern societies also have new crimes that target evolved harms, such as antitrust and environmental violations.

Cybercrime, like crime, consists of engaging in conduct that has been outlawed by a society because it threatens social order. Cybercrime differs from crime primarily in the way it is committed: real-world criminals use physical tools—such as guns—to commit their crimes; cybercriminals use computer technology to commit cybercrimes. As we will see in the next chapters, most of the cybercrime we see today simply represents the migration of real-world crime into cyberspace. That is, cyberspace becomes the tool criminals use to commit old crimes—like fraud, theft, and extortion—in new ways.

Their use of computer technology does not fundamentally alter the nature of the activity at issue; fraud is fraud, whether committed online or off line. But while the result—the harm—may be the same, the criminal activity is not. The use of computer technology impacts the commission and investigation of these crimes in ways of which the law has been required to take cognizance.

Criminals' use of computer technology lets them commit crime on a scale far exceeding what is possible in the real world; the magnitude of the harm cybercrime causes is therefore one factor that differentiates crime and cybercrime in ways the law must address. Another differentiating factor is that the use of computer technology makes it difficult—and often impossible—for law enforcement officers to identify and apprehend those responsible for cybercrimes. Finally, all cybercrime does not merely represent the commission of traditional, core crimes by new means: all cybercrime is not simply the online replication of old crimes; there are new, distinct cybercrimes, and more might emerge in the future.

The Cybercrime: Kentucky, 2009

In the last full week of June 2009, cybercriminals operating from outside the United States surreptitiously extracted $415,989 from an account at the First Federal Savings Bank in Shepherdsville, Kentucky.[5] The account belonged to Bullitt County; it held funds the county used to pay its employees.

On June 22, "someone started making unauthorized wire transfers of $10,000 or less from the county's payroll to accounts belonging to at least

25 individuals around the country."[6] It was not until June 29 that First Federal Savings Bank employees "realized something was wrong"; once they realized the transfers were unauthorized, First Federal employees froze the account and contacted banks that had received transfers, asking the banks to reverse them.[7] And it was on June 29 that a First Federal employee called Melanie Roberts, the Bullitt County judge-executive who was one of the two people authorized to initiate fund transfers from the county's account, to tell her about the unauthorized transfers.[8]

Since no one in Bullitt County had any idea who was responsible for the transfers, county officials contacted the FBI, which began an investigation.[9] The investigation showed that the unauthorized transfers—the thefts—originated in Ukraine, a country known to be a base of operations for cybercriminals.[10] The cybercriminals responsible for the Bullitt County thefts used a sophisticated scheme to bypass the security measures the county and the bank had put in place to prevent the kind of unauthorized transfers that occurred in this case. Since the tactics these cybercriminals used illustrate the technical sophistication typical of contemporary cybercrime, it is useful to analyze this particular scheme in some detail.[11]

Bullitt County used a dual-authorization system to protect the five accounts it maintained at the bank; wire transfers of funds had to be authorized by two county employees—the county treasurer and the county judge-executive. The treasurer initiated transfers, and the judge-executive approved them. The bank relied on several methods to protect the funds for which it was responsible, one of which was to use special programming to analyze customers' computer systems and "create a unique fingerprint" of their computers.[12] This meant that if a cybercriminal tried to log into a customer's account from a computer other than the one the customer routinely used, the bank's system would detect that because the "fingerprints" of the two computers would not match. When the bank's system detected that a log-in attempt was being made from a computer with an unknown fingerprint, it would not allow the log-in and would send the owner of the account an e-mail that contained a "one-time passphrase"; the customer would have to enter the passphrase, along with her or his username and password, to access the account.

The cybercriminals responsible for the Bullitt County thefts used a Trojan horse program known as Zeus to bypass both the county's and the

bank's systems. They "somehow got the Zeus Trojan" on the treasurer's computer and "used it to steal the username and password" she needed to access e-mail and the county's accounts at the bank.[13] Zeus installs itself on a computer's hard drive and steals banking information by recording keystrokes typed on the keyboard; it uses an instant message to send the information to the cybercriminals who control it. Zeus also "creates a direct connection" between the infected computer (here, the treasurer's computer) and the system used by the cybercriminals; this lets them "log in to the victim's bank account using the victim's" own computer and Internet connection.[14]

The thieves began by stealing the treasurer's username and password and linking her computer with the one they would use in the thefts. Then they logged into the county's bank account by "tunneling through" the treasurer's Internet connection.[15] Since they were using her Internet connection, the bank's fingerprinting system did not flag this as a problematic attempt to log into the account. Once they were logged into the payroll account, the thieves changed the password the judge-executive would have to use to log into the account and changed the e-mail address associated with her access to the account. The next thing they did was to create "several fictitious" county employees and "a batch of wire transfers to those individuals" that would need to be approved by the judge-executive. We will come back to the fictitious employees in a moment.

After they initiated the wire transfers, the cyberthieves logged into the county's payroll account using a computer outside Kentucky and the new e-mail address and password they created for the judge-executive. When the bank's system did not recognize that computer's fingerprint, it sent an e-mail with the passphrase the judge-executive would have to use to log into the payroll account and approve the transfers. The e-mail went to the new e-mail address the thieves had substituted for the correct one—an address they controlled. The thieves retrieved the passphrase, logged into the account with the judge-executive's new e-mail address and password, plus the passphrase, and approved the unauthorized wire transfers. Since there was nothing ostensibly problematic about the transfers or the process used to approve them, it is not surprising that it took the bank a week to realize something was wrong.

Where did the transferred funds go? Weeks before the thieves compromised the treasurer's and judge-executive's computers, they hired twenty-

five individuals to serve as "money mules," unwitting dupes who would receive transfers from the county's account and then unwittingly pass the money along to the thieves. The thieves hired at least some of the mules after finding their resumes on Careerbuilder.com. The Fairlove Delivery Service hired the mules to edit "documents for grammar" and promised them they would be paid eight dollars for "each kilobyte of data they processed."[16] One mule said that, after she edited text for a while, she asked when she would be paid. In response, she received an e-mail asking if she would be interested in becoming a "local agent" for the company; she was told it "had trouble getting money to its clients overseas as quickly as they needed it, and desperately needed help speeding up that process."[17] After she agreed, she received a wire transfer of over $9,900 and was told to wire all of the money except for her 5 percent "commission" to a bank account in Ukraine.[18] She was suspicious and so "only wired $3,000 of the money."[19] Other mules wired all money they received except for their "commissions." If their banks reversed the fraudulent transfers (as some did), these mules found themselves owing Bullitt County the money they wired to Ukraine.

What happened to the money that went to Ukraine and to the thieves that received it? Basically, nothing happened; the money presumably sits in accounts in Ukraine or in whatever country to which it was subsequently transferred. The only money the county recovered came from the U.S. banks that froze accounts or reversed the fraudulent transfers. The county sued the bank, claiming that the bank's negligence was responsible for its losses and that the bank is therefore required to reimburse the county for the $415,989 it lost.[20] The bank denies it was negligent; it claims the county was at fault for not having caught the unauthorized transfers.[21] The suit is pending. And none of the cybercriminals who siphoned nearly $416,000 out of Bullitt County's payroll account has been identified or apprehended—and as we will see in chapter 6, none are likely to be.

Implications of the Bullitt County Case

What happened in Bullitt County, Kentucky, in the summer of 2009 illustrates how and why cybercrime challenges lawmakers and law enforcers in the United States and elsewhere.

Unlike traditional crime, cybercrime tends to be a low-risk, high-

reward endeavor for those who engage in it. The Bullitt County incident perfectly illustrates both characteristics of this new type of crime.

The reward is obvious: a group of cybercriminals (identities and location unknown) got away with almost half a million dollars in one criminal episode, which almost certainly was not, and will not be, their only foray into cybercrime. This is far from an isolated incident: in 2007, cybercriminals (variously described as Germans or Ukrainians) used similar tactics to "hijack $6 million from banks in the United States, United Kingdom, Spain and Italy."[22] And in the summer of 2010, unidentified perpetrators used the Zeus Trojan horse program and tactics similar to those involved in the Bullitt County theft to steal more than one million dollars from banks in the United Kingdom.[23] An unknown number of similar bank thefts have occurred since and are occurring as I write this (and, no doubt, as you read it), along with other types of financial cybercrime. In 2009, the FBI told Congress, "Revenues from cybercrime [had] reached an estimated $1 trillion per year."[24] This figure probably understates the actual amount cybercriminals reaped and victims lost that year; as we will see, businesses are very reluctant to report being victims of cybercrime for fear their customers will lose confidence in them.

The low risk of being apprehended is perhaps less obvious but no less significant: the unknown Bullitt County perpetrators have not and almost certainly will not be apprehended and brought to justice for the theft of Bullitt County's funds. Cybercriminals who operate domestically are likely to be apprehended, but those who operate transnationally run little risk of being apprehended and punished for their crimes. One reason for the difference is the difficulty of tracing the actual location from which offshore cybercriminals operate; the Bullitt County thieves were suspected to be in Ukraine, but they might have routed the signals they used to hack the treasurer's and judge-executive's computers and the county's account through Ukraine in order to hide the fact that they were actually operating from, say, Brazil. Tracing the origin of a cybercrime is a difficult and time-consuming process, one that is often beyond the capacity of local law enforcement agencies. And even if Bullitt County law enforcement officers—with, perhaps, the assistance of the FBI—were able to trace the cyberthieves to Ukraine, they would somehow have to be able to take them into custody. The United States does not have an extradition

treaty with Ukraine,[25] which means Ukraine would not be obliged to turn the cyberthieves over to U.S. authorities for prosecution.

A third factor that differentiates cybercrime from traditional crime is the crime scene: The legal and practical challenges involved in investigating the Bullitt County thefts and apprehending those responsible for them are exacerbated by the fact that this cybercrime, like all cybercrimes, involved digital evidence and a virtual crime scene. As we all probably know from books, movies, and television shows like *CSI: Miami* and *Law and Order*, the investigation of a crime focuses on the place where it was committed: the crime scene. In traditional, real-world crimes—robberies or murders, say—the crime happens at one physical location; officers carefully scrutinize that location for trace evidence they can use to identity, locate, and convict those responsible for the crime. In cybercrimes, the crime scene—and any attendant trace evidence—is scattered across multiple locations, for example, the location from which the perpetrator(s) operated, the location where they inflicted harm on the victim, and the intermediate locations through which the bits and bytes involved in the commission of the crime traveled between perpetrator(s) and victim.

In the Bullitt County case, the crime scene was scattered across at least two continents: digital evidence existed in the county treasurer's and judge-executive's computer systems, in the bank's computer system, in the Ukrainian computer systems involved in the crime, in the mules' computers, and in all of the computers in the United States, Ukraine, and other countries through which the signals involved in consummating the crime traveled as it was carried out. This means the process of putting the crime together and assembling the evidence needed to convict the perpetrators will be extraordinarily complex and therefore must be carried out by those with expertise in digital evidence and digital investigations. Bullitt County may have investigators with some experience in digital evidence, but it probably does not have individuals with the type of expertise needed to unravel a transnational cybercrime of this complexity. The FBI was, as we saw earlier, called in to assist with the investigation, but the FBI can only do so much because it has other investigative priorities (e.g., terrorism) and because it is a comparatively small agency with limited resources.

Cyber Bonnies and Clydes

Cybercrime is not the first instance in which criminals have exploited new technology to their advantage. David Ronfeldt and John Arquilla found that the "bad guys" tend to be among the first adopters of innovative technologies and techniques because they are not constrained by existing rules and procedures.[26] This tendency manifested itself in the 1930s, when law enforcement officers found themselves dealing with criminals who used automobiles (still a relatively new technology) to increase their chances of committing financially rewarding crimes such as kidnapping and robbery without being apprehended and punished.

Automobiles gave criminals a distinct advantage in countries like the United States that use a federal governance system. They could "plan a crime in one state, execute it in another, and then return to the first state or hurtle into some other remote locality for the hiding-out . . . period."[27] Bank robbers, car thieves, kidnappers, pimps, and other criminals quickly realized they could frustrate law enforcement efforts to apprehend them if they used motor vehicles to flee a state after committing a crime there. They understood the importance of the technology. In 1934, Clyde Barrow, of the Bonnie and Clyde gang, wrote a letter to Henry Ford, thanking him for his "steel-bodied V-8 automobiles" because they made it so much easier for the gang to elude police after they committed a robbery.[28]

There were several reasons automobiles made it easy for Bonnie and Clyde and their various colleagues in crime to avoid capture. The most obvious is the one noted above, that is, once criminals who had, say, robbed a bank in Indiana crossed the border into Illinois, Indiana police no longer had jurisdiction to arrest them and the Illinois police had no jurisdiction because no crime had been committed in their state. If the Illinois police captured the robbers, there were procedures by which they could be extradited to Indiana for prosecution, but the procedures were complex and took time; and while extradition was pending, the criminals might disappear into yet another state or disguise themselves so the Illinois police would not be able to find them. Also, the Illinois police might not put a great deal of effort into investigating a crime that had been committed outside their jurisdiction.

Cybercriminals substitute cyberspace for the automobile: like the vehicles Bonnie and Clyde relied on, cyberspace lets cybercriminals exploit

jurisdictional boundaries to avoid being apprehended and punished for their crimes. That was the only advantage automobile technology provided for the motorized criminals of the 1920s and 1930s.

Cyberspace, on the other hand, provides other advantages: perhaps the most obvious is that cybercriminals do not have to physically enter the territory of the sovereign entity where they commit their crimes; as we saw above, Ukrainian cybercriminals can rob banks in other countries without ever leaving their homes. That exacerbates the impact of the jurisdictional avoidance technique noted above, which was effective but far from foolproof. Some of Bonnie and Clyde's bank-robbing colleagues—including John Dillinger—were captured and briefly imprisoned for their crimes. Since cybercriminals do not have to physically enter the territory of the jurisdictions in which they commit crimes, their use of cyberspace dramatically reduces the likelihood they will be identified and apprehended.

Cyberspace also provides criminals with yet another advantage: anonymity. Even if the bank robbers of the Bonnie and Clyde era wore masks as they committed their crimes, they were easily identifiable as they fled the scene of the crime. Locals were likely to notice a strange vehicle speeding out of town, and the employees of gas stations and cafés were equally likely to notice strange people who stopped for food and fuel. Bonnie and Clyde and their bank-robbing colleagues era might escape the scene of the crime, but they could not escape being identified, which ultimately tended to result in their being arrested. Cybercriminals never physically enter the territory where they commit their crimes; no one observes their appearance, and they leave no traces of their physical existence at the crime scene. They also eliminate the need to flee a physical crime scene; they terminate their involvement with the digital scene of their crime by shutting down their computer or simply moving on to the next victim.

My purpose is to illustrate a simple, yet foundational, principle: cyberspace is a criminal tool of unprecedented complexity and potential. As a result, lawmakers and law enforcers are waging a losing battle against cybercrime because cyberspace lets cybercriminals evade the laws and tactics nation-states have devised to deal with unlawful conduct. In the chapters that follow, we will review precisely how and why cyberspace is such an exceptional criminal tool and what lawmakers and law enforcers are doing in an effort to nullify its utility in this regard.

A Framework for Examining Cybercrime and the Law

The discussion of cybercrime in the following chapters utilizes a distinct conceptual framework that was developed as a tool for analyzing cybercrime.[29] "Cybercrime" is the term lawyers and law enforcement officers use to refer to crimes the commission of which involves the use of computer technology. This conceptual framework divides cybercrimes into three categories: (1) a computer is the target of the crime (often a new cybercrime); (2) a computer is a tool used to commit a traditional crime such as theft or fraud; and (3) a computer plays an incidental role in committing one or more crimes.[30]

A computer is the target of criminal activity when the perpetrator attacks the computer by breaking into it, introducing code that damages it, or bombarding it with data. Here, the computer is essentially the victim of the crime. Access target crimes involve accessing a computer without being at all authorized to do so (the outsider cybercrime) or by exceeding the scope of one's authorized access to a computer (the insider cybercrime). U.S. cybercrime statutes usually define "access" as "to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or network."[31] Access can be an end in itself or it can be used to commit another crime, such as damaging or stealing data from the computer. Access target cybercrimes are examined in chapter 1.

Code target crimes involve creating, disseminating, and using malware, computer viruses, worms, and other malicious code that damages a computer system or extracts data from it.[32] Data target crimes involve blasting a computer linked to the Internet with so much data it essentially goes off line in what is known as a distributed denial of service (DDOS) attack; the target computer receives so many malicious signals from the attacker that no legitimate traffic can reach it.[33] Code and data target crimes are examined in chapter 2.

A computer can also be a tool to commit a traditional crime, such as theft or fraud. Here, the computer's role is analogous to the role a telephone plays when a fraudster uses it to trick victims into parting with their money or property. In both instances, the use of a particular technology facilitates the commission of the crime but does not alter the nature of the offense. Computers can be used to commit most traditional crimes, in-

cluding fraud, embezzlement, theft, arson, forgery, riot, assault, rape, and homicide. Tool cybercrimes are examined in chapters 3 and 4.

Finally, a computer can play an incidental role in the commission of a crime. This alternative encompasses a variety of activity, such as blackmailers using computers to e-mail their victims and drug dealers using computers and Excel to track their inventory and drug transactions. In these and similar instances, the computer's role in the crime is as a source of evidence, nothing more. That role, however, can be important; computers can, in effect, become the crime scene. The evidence investigators find on drug dealers' computers may play an essential role in convicting them of the crimes. This aspect of cybercrimes is examined in chapter 5.

This trichotomy plays two roles in analyzing cybercrimes: Investigators use it to assess how they should draft search warrants and otherwise incorporate computer technology into their investigative process. And judges and legislators use it to determine if existing law is adequate to criminalize how a computer was used in a given instance; if it is not, then judges and legislators may need to extend the reach of existing law or adopt new law.