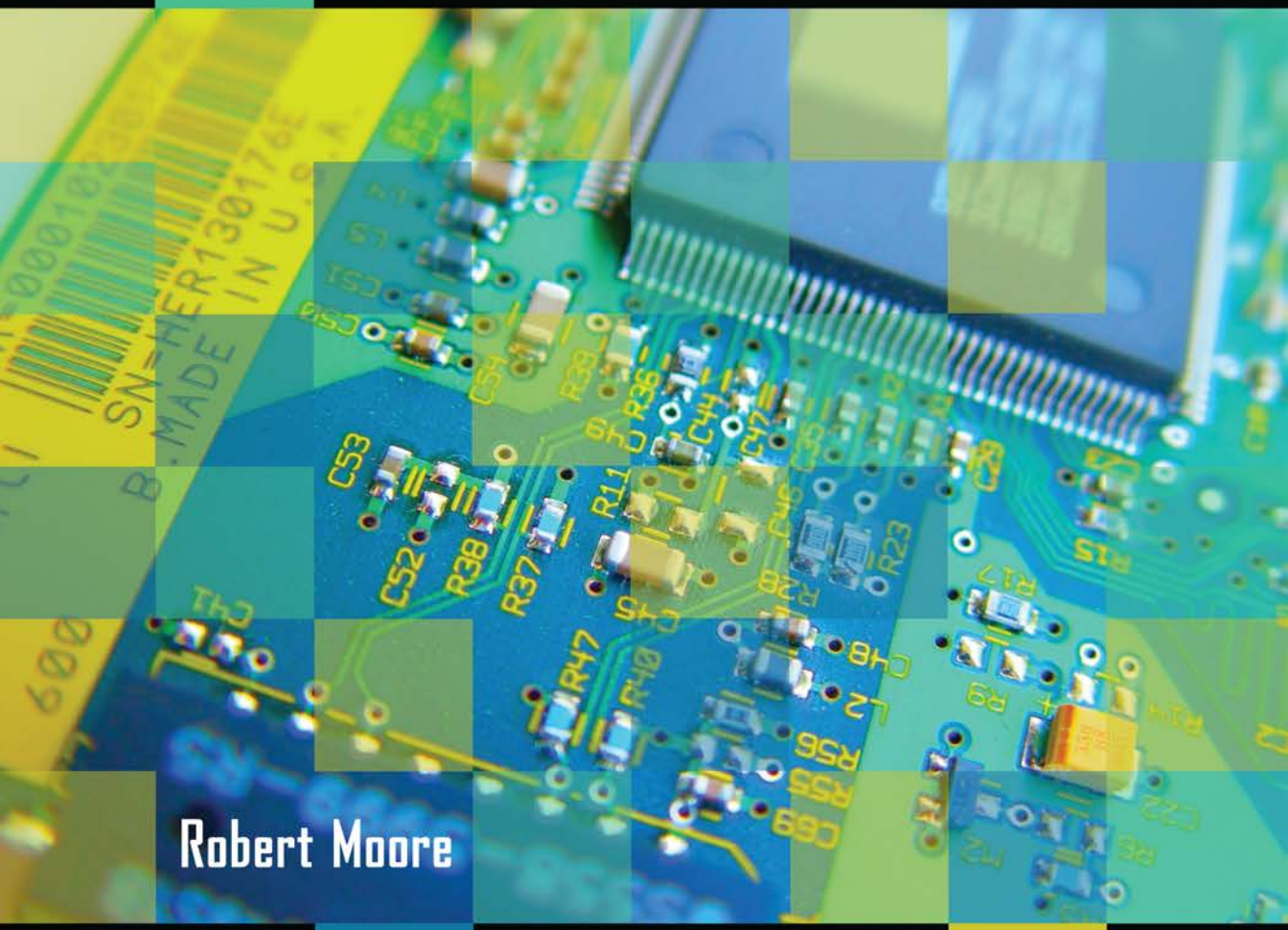
CYBERCRIME

investigating high-technology computer crime



Robert Moore

second edition

ROUTLEDGE

CYBERCRIME

INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME

SECOND EDITION

ROBERT MOORE

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First Published 2011 by Anderson Publishing

Published 2015 by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017, USA

Routledge is an imprint of the Taylor & Francis Group, an informa business

Library of Congress Control Number: 2010935324

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-1-4377-5582-4 (pbk)

Table of Contents

Introduction

The topic of high-technology crime and cybercrime is discussed much more today than it was five years ago when the first edition of this text was released. Computers have become integral parts of the daily lives of citizens around the world. The number of individuals who gain access to the World Wide Web, both for legitimate and for illegitimate reasons, continues to increase every day. Criminal activities involving computers and technology continue to be a problem for the criminal justice system. It is worth noting that while crime numbers have increased over the last five years, the criminal justice response has also increased. Today there are more criminal justice agencies staffing cybercrime-related investigators. Additionally, there are more computer forensics services available for investigators. However, there is still a continuing need to increase awareness and understanding of cyber-related crime.

There is an incredible amount of literature on the topic of cybercrime, ranging from works on cybercrime in general to more specific works that focus on particular cyber-related crimes. However, the current work seeks to continue its original goal—to provide an introductory level of coverage to a rapidly changing field of the criminal justice system. This work is written for those who have limited or no knowledge of how computers work and/or computer networking principles. Readers are introduced to various complex topics in an easy-to-understand format. It is the hope of the author that these materials can be of use not just to university students but also to those who are currently working in the criminal justice field.

The book is divided into three sections. The first section consists of an introduction to high-technology crime, which is also commonly referred to as *cybercrime*. The second section addresses investigative issues associated with the investigation and prosecution of these crimes. The final section provides readers with some insight into the future of study in the area of high-technology crime, including current issues and an introduction to the emerging field of cybercriminology.

It is not the intent of this work to make the reader an expert in the area of high-technology crime, for no single work could accomplish this. The

field is complex and constantly changing, as the technology used by both the criminals and the criminal justice system continues to evolve. Instead, the reader should view this work as a starting point for future study and research on the topic. To assist in this process each chapter concludes with a series of review questions designed to highlight the important terminology and concepts presented within each chapter. Each chapter also contains reference to related books, articles, or court cases that have been selected to provide interested readers with a means of continuing their education in this area. There are also a variety of websites and organizations that maintain a virtual presence on the World Wide Web, many of which provide up-to-date information on many of the topics discussed in this work. Therefore, each chapter will contain a brief listing of relevant websites that readers may visit in order to continue learning about the topics addressed in each chapter. Finally, every chapter except the final one will contain a brief spotlight on a news story that addresses how the materials discussed in the chapter are used or encountered in practice. These news stories are relatively recent; the stories come from news sources within the previous two to three years, with the majority published in the year before press time. The final chapter covers the new and exciting area of cybercriminology. Scholars in this area of study are working to gain a better understanding of what causes individuals to engage in the many cyber-related crimes that are discussed in this work. While there are few news articles that address these studies, numerous academic journal articles and textbooks are being developed on the topics, and readers are provided with information on these works.

As with the first edition, it is the hope of this author that this work will motivate readers to become more involved in the areas of research and training in the high-technology crime field.

Chapter 1

An Introduction to High-Technology Crime

When discussing crimes that involve computers and technology it is possible that prior to this reading the term *high-technology crime* may not have been heard by the reader. The term *technology* is often used to refer to mechanical or electrical devices that assist individuals in their day-to-day activities, but what does it mean to discuss *high technology*? As this is a work designed for those who are either interested in or currently involved in the field of criminal justice, let us take the standard equipment of a law enforcement officer as an example. Today, most all law enforcement personnel carry a firearm of some type, regardless of whether they elect to utilize a revolver or a semi-automatic. Is the officer's firearm a piece of technology? Of course. The firearm is a highly mechanical device, with the revolver having been developed by Samuel Colt in 1836. Therefore, the firearm is a piece of technology and one that has been around for more than a 100 years. Now, is the firearm a piece of high technology? This could be debatable, as some would consider the complex designs and manufacturing components of the firearm to make it a highly sophisticated piece of technology. But does being highly sophisticated equate to being considered high technology? Probably not. In the eyes of this author, the term *high technology* invokes images of highly developed electronic devices—more in line with the components that make up a cellular telephone than the components of a firearm.

It is worth noting that for many people what they consider to be a computer—the large electronic device that we type our research papers on and use to browse the Internet—is not the limitation for the technology. A computer is an electronic device that allows the user to input information, process that information, and then receive

DOI: 10.1016/B978-1-4377-5582-4.00001-7

results that are based on the information provided by the user. Many of these devices do not come with monitors or keyboards. For example, many of us now commonly use a debit card at the local convenience store, thereby saving us the time and effort it takes to write out a check. To complete our financial transactions, the cashier merely takes our debit card and swipes the magnetic strip through a small machine, returning our card to us when he or she is finished. The small device attached to the cashier's cash register will obtain our account number from the magnetic strip on the back of the debit card. We as users then enter our PIN onto the keypad, and the transaction is either approved or rejected. The machine that reads our debit cards is a miniature computer. Furthermore, the debit card scanner would meet our earlier established criteria for being considered an example of a high-technology device. Another example of technological devices seeing increased use in our society would be cellular telephones. In the five years since the first edition of this text was published, a number of cellular phone manufacturers continue to release phones containing increasingly advanced software applications. Today's cellular phone can allow users from around the world to input information, process information, and send or receive information almost instantaneously. Each of these devices is a highly sophisticated electronic device that would therefore meet the previously discussed definition of a high-technology device. Now that we have a basic understanding of some examples of high-technology devices, questions that remain involve gaining a better understanding of high-technology crime and determining whether such criminal behavior is a serious problem that truly warrants examination and consideration.

What Is High-Technology Crime?

In keeping with the definition of high technology previously noted, *high-technology crime* refers to any crime involving the use of high-technology devices in its commission. These are crimes that involve the use of computers, telephones, check-reading machines, credit card machines, and any other device that meets the previous definition of high technology. There are numerous forms of high-technology crime, ranging from traditional crimes committed prior to technological advances, to newer crimes that rely on high-technology devices to commit crimes. In the past, there have been several different ways of referring to crimes involving high-technology devices. Perhaps the two best-known classifications used to distinguish these crimes are computer crimes or cybercrimes.

Computer Crimes

Traditionally, the term *computer crime* has been used to refer to criminal activities involving a computer that are made illegal through statute. The definition espoused by Eoghan Casey, one of the most well-known researchers in the area of computer-related crime, is used here because of the clarity of his focus. Accordingly, a computer crime would be a crime that involves a computer in one of the following ways:

- *The computer as an instrument of the crime.* Here, the computer is used as a means of engaging in the criminal activity. Under this category, the crime cannot be committed without the computer being turned on and used in the commission of the act. An example here would be the individual who uses a company computer to embezzle funds from a company account.
- *The computer as the focus of a crime.* Here, the computer is the intended target of criminal activity and is not necessarily used in the commission of the act. The best example of this is the individual who breaks into a computer supply store after hours with the intention of stealing computers and computer peripheral equipment.
- *The computer as a repository of evidence.* Here, the individual involved in a criminal act has not stolen the computer and has not used the computer as a means of committing the criminal act, but he or she has stored evidence on the machine. A good example of this is the individual who stores his or her illegally copied music files on his or her home computer. Note then that for this category to be applicable, the storage computer could not have been involved in the criminal activity. However, the generalizations are of minor concern because regardless of which category or categories the individual's actions fall under, she or he is still guilty of a computer crime under this definition.

This definition is a good means of addressing criminal activities that involve computer technology. Let us examine one of the more famous and commonly read about computer crimes: hacking. *Hacking* refers to the unauthorized access of another person's computer, and would be considered a computer crime under the preceding definition for several reasons. First, the crime involves a computer that was used as an instrument of the crime. To be guilty of hacking, one must actually type in commands to penetrate the security of a second computer. Second, both computers will probably maintain some form(s) of evidence that could be used to

confirm the identity of the hackers. As such, computers involved in hacking would meet the third definition above, whereby computers are repositories of evidence related to a crime—in this case, the crime of hacking into the target computer.

Cybercrime

Cybercrime, returning to a definition provided by Casey, refers to any crime that involves a computer and a network, where a computer may or may not have played an instrumental part in the commission of the crime. The term *cybercrime* would be used to refer to a criminal act like that of identity theft, which involves the theft of someone's personal information such as their credit card number or Social Security number. When an individual commits the crime of identity theft, there are several methods of obtaining a target's personal information. Many of the techniques involve the use of a computer or a network, but many more techniques have nothing to do with computers other than information stored in text files on a computer's hard drive.

In reading the discussion above it becomes clear that the term *cybercrime* actually refers to computer-related crime; however, some consider computer crime to be a subdivision of cybercrime that warrants its own definition and understanding. The determining factor between the two appears to be little more than the issue of whether a statute is present to criminalize the use of the computer in the criminal act. Because of the fact that more crimes today are relying on the Internet, there has been a significant effort by legislators to expressly criminalize these acts in the statutes. For example, as recently as 10 years ago, many states did not criminalize online harassment. Apparently, the reigning thought at the time was that harassment via the computer did not have the necessary psychological or physical impact necessary to show harm to an individual. Legislators and criminal justice professionals today are beginning to understand the dangers of such crimes. Prior to the enactment of these statutes, individuals guilty of harassing someone over the Internet were prosecuted under other statutes that were, for lack of a better term, "stretched out" to include the crime under investigation. Now that more of the crimes are being made illegal through express statutes, the question arises as to whether there is a need to differentiate between the two forms of crime. Should computer crime be considered separately from cybercrime? After all, over the last five years the term *cybercrime* has superseded that of *computer crime*. A quick search for book and journal articles on the topic of cybercrime versus the topic of computer crime would result in a confusing number of articles as more researchers and professionals are utilizing the term *cybercrime* as an umbrella term for all crime involving computers and technology.

Consolidating High-Technology Crimes

It could be argued that criminal behavior is criminal behavior regardless of the terminology used to describe the behavior. Therefore, a strong argument could be made that the distinction between a computer crime and a cybercrime is trivial. Both activities are crimes, and both activities involve technology in the commission of the acts. The majority of hacking attacks, with hacking being the most historically well known of computer crimes, are now reliant on the Internet and network connections. Because of this fact, the definition of a computer crime is now beginning to blur into the definition of a cybercrime—being that the worldwide network, the Internet, is now involved in many criminal activities that rely on computer technology.

In this work, I hope to provide information on several crimes that may involve only limited influence of computers and networks, as well as acts that rely almost entirely on the use of a computer and a network. These crimes most often involve highly developed technology in the commission of the crime, and as such the term *high-technology crime* is utilized for the purposes of this work. By utilizing this term I am referring to criminal activities that may have at one time been considered a computer crime or a cybercrime, with some of the crimes being considered a combination of both. Semantics regarding whether the act is a computer crime versus a cybercrime versus a high-technology crime is not important. Gaining a better understanding of the problem and the need to develop a strong response is more important.

How Serious Is the High-Technology Crime Problem?

With the term *high-technology crime* we are now referring to many diverse criminal activities such as hacking, digital child pornography, identity theft, intellectual property theft, and online fraud. The rate of each of these crimes has been steadily increasing in recent years and, when examined as a whole, amounts to a very serious problem. It should also be noted that the problem is not isolated to the United States. Problems associated with high-technology crimes have become increasingly more discussed in every country around the world—even in countries not known for their high levels of technological development and skill. Technology has played a key role in globalization, but this shrinking of the world has also led to many difficulties in terms of criminal activity. The worldwide nature of high-technology crime has developed problems involving such considerations as jurisdiction. In some cases it is now very difficult to determine who has the authority to investigate a high-technology crime. For example, an individual living in Russia is capable of transmitting an image of child pornography here to the United States. In this situation, who has

jurisdiction? Russia? Perhaps under Russian law the young girl in the picture was of legal consenting age. Was there then a crime committed in the eyes of Russian law enforcement personnel? Does the United States have jurisdiction? It is illegal to transmit images of juveniles, but the individual never touched U.S. soil when committing the criminal act. Can the use of American telephone lines be considered when examining whether there is jurisdiction for an investigation? These are all important questions that are not easily answered. There is, however, an increasing level of debate and intelligent discussion among world leaders as more international entities are coming to recognize the dangers of high-technology crimes.

The increasing frequency of the crimes alone is enough to justify a certain level of concern. According to data released by the Internet Crime Complaint Center, complaints of fraud and attempted network intrusions were up 33.1 percent for the year 2008 compared with data from 2007. Many of these reported cases involved online fraud, with the median loss being $931.00 per complainant. For further proof of the problem, one has to look no further than his or her local or national newspapers. It seems that rarely a week goes by without there being a report of some form of high technology–related crime happening around the country. Many of these reports concern credit card accounts being hacked or a new computer virus being released. The release of computer viruses and the constant need to prevent unauthorized access to vital information has led some companies to hire individuals whose sole job is writing antivirus software programs or defending computer networks against outside attackers.

While hacking was historically the most recognized high-technology crime, it is not the only crime seeing increased reporting and prosecution. Digital child pornography, to be discussed more fully in Chapter 4, is unfortunately increasing. Child pornography is a troubling crime if for no other reason than the fact that children are sexually abused in the manufacturing of the materials. According to one federal law enforcement official, as much as 50 percent of all cases involving computers and technology are child pornography cases. Some state law enforcement agencies put the numbers as high as 75 percent, meaning that three out of four high-technology crimes involve the manufacture, distribution, or possession of child pornography. This becomes especially important when one considers that increasingly more states are being asked to handle their own high-technology crime investigations as the federal government shifts its focus to other areas of criminal jurisdiction.

Another high-technology crime that has seen a dramatic increase in reporting is identity theft or online fraud. According to information provided by Equifax, one of the leading credit reporting agencies in the United States, identity theft has affected more than 27 million Americans over the last 5 to 6 years. These figures are even more astounding when one considers that many individuals do not report their victimization because they

either do not understand the crime or do not realize that they have been victimized until they go to apply for credit. Identity theft is perhaps such an attractive crime because it is possible to commit the crime and move on before the victim even realizes he or she has been victimized.

The frequency of high-technology crime is also presenting a problem for law enforcement personnel because of the need for training and equipment. While recognition and response to the problem is better today than it was 10 years ago, there are still many law enforcement agencies that face the same problem year after year—a budget shortfall. The budgetary issues are especially problematic for smaller police and sheriff's departments in rural communities. Criminals may retreat to these smaller communities when they want to get away from the larger cities in hopes of being able to stay outside the reach of law enforcement. The funds necessary to investigate high-technology crimes are significant, if for no other reason than the training. Take, for example, the following scenario concerning drug trafficking:

> A major narcotics trafficking operation is believed to be operating out of a county with a population of 22,000. The local sheriff and police chief have worked together to investigate the individuals believed to be involved. However, there has been no communication between the suspects and any buyers. During a routine suicide investigation involving an individual believed to have been a part of the narcotics operation, a deputy encounters a personal computer in the subject's bedroom.

In the above example, the deputy probably would not consider taking the computer back to the department for examination. Further, if the computer was taken, there is the possibility that the department would not have a deputy capable of examining the computer for evidence; in fact, it is highly probable that the department would not have a deputy capable of forensically examining the computer. What evidence could the computer contain? Remember that no one has been able to monitor a telephone communication concerning a narcotics transaction. The information is obviously being conveyed somehow. Perhaps the individuals are using electronic communications to facilitate their transactions. As foreign as this idea sounds, it is in fact becoming a more common occurrence in the drug trade industry. Because smaller departments either do not think about or know how to monitor e-mail, more narcotics organizations may rely on the technology as a tool for arranging drop times and locations. Even more interesting is the consideration of whether the computer could be used to prove whether the individual was murdered or committed suicide. Perhaps the individual did not commit suicide, and evidence on the computer could be used to corroborate this claim. Another scenario, which I encountered many times when working narcotics-related cases, would involve the collection of evidence from cellular telephones.

Because today's cellular phones are more like miniature computers, they are capable of storing vast amounts of information in the form of e-mails, text messages, videos, or still pictures. These devices are often seized and examined to obtain call logs, but what about other forms of digital evidence?

The Purpose of This Work

There is no way this work can remove the financial roadblocks involved in investigating high-technology crime. However, hopefully the materials presented here can provide a starting point for investigators, students, and private citizens who may come into contact with these crimes, or perhaps for individuals who maintain an interest in these areas of crime. As stated earlier, the problems associated with high-technology crime are increasing every day. While historically it was possible for an individual to indicate that he or she was not interested in investigating high-technology crimes, today's criminal justice personnel have no such luxury. It is no longer a question of whether a law enforcement official will encounter a criminal act involving a high-technology device, but rather a question of when and how often such an encounter will take place. The goal of this work is to provide readers with some basic information on how some of the more commonly encountered high-technology crimes are committed, as well as some of the more basic investigative strategies. The work is not written to make the reader an expert in the area of high-technology crime investigation, but the foundations for such training are laid within this work. To facilitate this level of understanding, the work will be divided into three sections: introduction to the criminal acts, introduction to the investigations, and introduction to computer forensics.

The Criminal Acts

Chapters in this section will focus on introducing the reader to the various criminal activities considered to be high-technology crime. The crimes included in this work are not exhaustive, but are instead representative of the crimes expected to be most commonly encountered by individuals in the criminal justice system. Each chapter will include a discussion on the nature and techniques associated with one or more high-technology crimes. Many of these crimes may be committed either with or without the computer, so a portion of each chapter may be designated to explaining the physical world techniques involved in committing the criminal act. Understanding the physical-world techniques is an important aspect of helping to understand how the individuals may apply the

information obtained from their physical-world exploits in furthering their criminal activities using the computer or the Internet. The following sections in this chapter present a more detailed overview of the material that will be covered in Chapters 2 through 12.

Chapter 2—Hacking and Phreaking

Hacking is arguably the most popular and well-known high-technology crime. This should not, however, be taken to mean it will be the most commonly encountered one. The technical nature of this activity results in this crime being one of the least-investigated criminal activities for nonspecialized investigators. Because hacking involves the unlawful access of another's computer without the legitimate owner's permission, the investigation requires a well-rounded understanding of computers and networking, or at the very least an advisor to help with understanding the complicated networking and computer protocols involved in the activity. *Phreaking* refers to the theft of telecommunications services and is discussed here with the crime of hacking because of the relationship the two have maintained in the past—historically a hacker would also likely be involved in phone phreaking, as one activity complements the other and assists in ensuring that the hacker remains unidentified.

The reader will be provided with a brief history of how hacking and phreaking have evolved over the past several decades, as well as how to distinguish among the various types of hackers. The tools and techniques employed by hackers will be briefly introduced in an attempt to provide information on the vast number of attacks possible given the current state of technology. The hacker/phreaker subculture will also be briefly discussed, as the language and terminology employed by these individuals is oftentimes confusing to those who have not been introduced to such communication style.

Chapter 3—Identity Theft

In this chapter, the reader is introduced to the crime of identity theft, which refers to the theft of another's personal identity, credit identity, or physical identity. Identity theft has been labeled as the fastest growing high-technology crime, and is one of the few high-technology crimes that originated without the use of advanced technology and still occurs frequently as a result of old fashioned con artistry rather than advanced technological skills. The evolution of physical-identity theft techniques will be discussed as a foundation for explaining how the Internet and technology have affected this criminal activity. While the crime still

occurs frequently in the physical world, even the physical activities can today involve several high-technology devices, and as such, this section will introduce the reader to information on how these crimes are accomplished. The section will conclude with an examination of the techniques used in committing identity theft via the Internet, and with information on identity theft in the future.

Chapter 4—Digital Child Pornography

While hacking is the best known and identity theft is the fastest growing, child pornography is regarded by many as the most physically damaging of the high-technology crimes. Child pornography is an old crime that has been modernized with the advent of technology. The Internet has revamped an industry built on human suffering that had begun to decline in popularity prior to the public release of the Internet. It has already been stated that child pornography is one of the most investigated high-technology crimes, but it is also one of the most debated. Returning briefly to our international crime example, there is a growing argument concerning the illegality of child pornography that is manufactured in a country where such materials are legal. Is it illegal to view child pornography? It is illegal to download and own child pornography, but what about the Internet user who stumbles across an international child pornography website? Are these individuals violating the law by looking at pictures on their screens? At what point does one own a digital image? These are all questions that are being asked around the world as the problem continues to get worse. Here in the United States, the issue has become even further clouded by recent Supreme Court decisions concerning the nature of privacy and child pornography. Today, it is necessary to not only prove that an individual owns an image of child pornography; it must now be proven that the image in fact depicts an actual child.

Chapter 4 will introduce the reader to this crime, including a brief history on child pornography and children's rights. More specifically, this section will provide the reader with information on what child pornography is used for; many people assume that the images are for personal pleasure, if one can consider such viewing pleasure. However, there are far more devious uses for images of child pornography, and these uses will be discussed in detail. The effect of digitization and the Internet will be discussed, as will be information on how the crime is committed today versus just a few short years ago. And lastly, the recent statutes and court decisions concerning the investigation of child pornography will be examined as a means of providing guidance for both those who are new to the field and those who have been investigating the crime for years.

Chapter 5—Internet Fraud

The term *Internet fraud* is rather broad, and therefore this chapter will be more of an overview of how the Internet has become a haven for fraudulent behavior in the 21st century. There are several crimes that qualify as Internet fraud, and each will be briefly introduced to the reader, with a discussion on how the crimes are committed and what can be done to prevent the crimes from growing in frequency. The first high-technology crime to be discussed here is that of online auction fraud. With the popularity of eBay and other auction websites, it should come as no surprise that fraud has become a popular issue in the past few years. Many individuals are now reporting that they are not receiving the merchandise for which they have paid. Another popular form of Internet fraud is that of adoption fraud; this crime is interesting because unlike auction fraud there may be a child up for adoption. The difference is that 10 or 15 individuals, with each paying upwards of $3,000 or more, may adopt the same child. The reader will then be introduced to one of the latest forms of fraud: the purchasing of wives online and online prostitution. Prostitution is said to be the world's oldest profession, and it has now moved onto the world's newest medium. Here, the reader will be introduced to how prostitution works on the Internet, and how potential "clients" are being defrauded every day. Finally, a brief discussion on how the Nigerian 419 scam, originally developed and enacted without the use of technology, has begun to increasingly rely on the use of e-mail as a means of locating potential victims. Each of the aforementioned crimes will be discussed so that the reader will be familiar with how the operations are conducted. Using this information, in conjunction with information presented in later chapters, individuals will be aware of how to handle a basic investigation involving one of these forms of crime.

Chapter 6—Online Harassment and Cyberstalking

Harassment and bullying have been topics of concern for professional educators and child care experts for years. However, more recently there has been a growing number of cases involving harassment via the Internet. One such harassment method involves the posting of negative or inflammatory remarks about a person on a social networking website such as Facebook or MySpace. With more than 350 million users and 200 million users, respectively, Facebook and MySpace have become tools used by harassers and bullies. A brief coverage of each of these programs and how online harassment is being conducted will be provided for readers in this chapter.

The second section of Chapter 6 will focus on the crime of cyberstalking. While closely related to online harassment, cyberstalking may become much more serious and dangerous should the stalking behaviors move from the Internet to the physical world. Cyberstalking as a crime is a relatively new concept, having been criminalized in many states only within the last few years, with some jurisdictions still failing to address the activity as a crime. In this chapter the reader will be introduced to information on how the crime occurs and why the crime is believed to be worthy of serious consideration by law enforcement personnel.

Chapter 7—Intellectual Property Theft and Digital Piracy

In this chapter the reader will be introduced to the crime of intellectual property theft. More specifically, this chapter will focus on discussing the crimes of digital file sharing and digital piracy. While these crimes are still not as often investigated by the criminal justice system, there is no denying that the activities have received international exposure and consideration. In much the same manner as child pornography, musical files and movies have undergone increased levels of digitization in the last decade. Today, thanks in part to the increasing size capacity of computer storage media and thanks in part to improved file compression software, it is now possible to store hundreds of movies or hundreds of thousands of songs on a computer storage device. These materials can then be traded via the Internet or via traditional methods, which involves the creation of digital video discs (DVDs). Again, while this particular criminal activity is not investigated as often by law enforcement personnel, the growing media coverage and use of the technology by otherwise noncriminal individuals dictates that a cursory coverage of the materials be provided.

Investigating High-Technology Crimes

In the second section, this work will focus on providing information relating to the actual investigations of the aforementioned crimes. The previous section provided the reader with information on how the crimes are committed and the current state of each crime in society. Here, the reader will learn how to actually begin taking steps toward the investigation of cases involving high-technology devices in the commission of a crime.

Chapter 8—Investigating Crime Online

In this section the reader will be introduced to online investigations, and more specifically online sting operations. Much like the investigation of traditional physical crimes, occasionally it will be necessary to conduct

a sting operation to ensnare suspects engaged in the commission of one of the aforementioned high-technology crimes. Here, the reader will be introduced to information related to establishing such operations. Additionally, the legal issues associated with online sting operations will be discussed, with special emphasis being placed on the issue of online entrapment. Because there may be little or no face-to-face interaction during the initial stages of establishing an online sting operation, it is necessary that investigators understand how the courts have ruled on investigations in general and on Internet investigations specifically. The recent popularity of online investigations by MSNBC's Dateline news program has led to many state and local law enforcement organizations developing an online presence to investigate reported instances of sexual solicitation of children.

Chapter 9—Search and Seizure of Digital Evidence

The Fourth Amendment of the U.S. Constitution states that unreasonable searches and seizures by law enforcement are forbidden. As part of this requirement, it is generally accepted that a search warrant be used when seizing evidence. All search warrants must be specific, but this specificity becomes increasingly important in regard to the seizure of digital evidence, which is merely the term used to describe evidence stored on a computer or other magnetic storage media. Here, the reader will be provided with information on drafting a search warrant, establishing the search warrant execution team, and pre-planning for the execution of the warrant. Just as the warrant must be more specific, the pre-planning for execution of a search warrant for digital evidence requires the investigator to ensure that certain aspects of the seizure will be properly handled during the initial moments following the beginning of the warrant's execution. This section will also include a brief examination of warrantless search doctrines and their application to the seizure of digital evidence.

Chapter 10—Executing Search Warrants for Digital Evidence

Unlike some other warrant executions, it is not enough to merely go in and collect the evidence listed on the search warrant. There are numerous additional considerations when the evidence to be seized is a computer or computer-related storage media. In this chapter, the reader will be provided with a step-by-step guide for executing a search warrant involving a computer or other high-technology device. Additionally, this section will include a discussion of how to protect the integrity of the evidence for instances in which the case goes to trial. According to some professionals, the majority of child pornography cases plead out because of either embarrassment or because they know there is sufficient evidence to

convict. Protection of evidence integrity may be instrumental in ensuring that the individual will plead guilty, but more importantly protecting the integrity of digital evidence will allow for the successful prosecution of individuals who do not plead guilty and proceed with a criminal trial.

Introduction to Computer Forensics and the Future of Technology Crime

In the third and final section the reader will be introduced to the issues of networking and computer forensics. This section has been included last as a means of providing a cap to the previously discussed issues. Here, the reader will be introduced to common networking concepts and terms, terms that will be beneficial to the investigator of high-technology crimes. Computer forensics is a relatively new field within criminal justice, and is one that is sure to see an increased level of support in the near future. Readers will leave this section with information on how the crimes are committed, how the crimes can be investigated and evidence seized, how networks may contain additional evidence, and how computer forensics can help solidify a case.

Chapter 11—An Introduction to Computer Forensics and Software

Computer forensics refers to the process of applying science and computers to the investigation of criminal acts. Here, the reader will be introduced to the field of computer forensics, with specific coverage of how the field has developed over the last several years and some of the more commonly used software packages. This chapter will also introduce readers to many of the legal issues associated with the capture and admission of digital evidence. The admission of scientific evidence into evidence for a criminal trial requires very specific criteria. This chapter will show readers how adherence to the computer forensics process can result in the proper admission of evidence during a criminal trial.

Chapter 12—The Future of High-Technology Crime

In this chapter the reader will be introduced to a couple of issues that I believe to be worth consideration in the near future. The first consideration involves the issue of cyberterrorism. While many debate the likelihood or possibility of another terrorist attack on American soil, there are some who claim that the next such domestic attack could involve a technology-based attack rather than a physical attack. In this section the

reader will be exposed to some of the more recent studies on cyberterrorism, including understanding what exactly is meant by the term *cyberterrorism*, as well as what techniques experts feel may be utilized by terrorists in the future. This chapter will then conclude with an examination of the role international law currently plays in the investigation and prosecution of high-technology crimes. Some of the problems, as well as some progressive international responses to the problem, will be discussed.

Chapter 13—An Introduction to Cybercriminology

In this, the final chapter, the reader will be provided with an introduction to the emerging field of cybercriminology—the study of why people engage in high-technology crimes. Many experts argue that complete eradication of high-technology crimes will be almost impossible. Because the technology, the techniques, and even in some cases the perpetrators change so much and so often, it is believed that the criminal behaviors will always stay one step ahead of law enforcement. This belief has led some to speculate that the future to fighting high-technology crime may lie in the education of younger generations who have the potential to make necessary changes. With this in mind, this chapter will introduce the reader to some studies associated with the application of traditional criminological theories to high-technology crime, as well as the development of new criminological theories associated with understanding high-technology crime.

IN THE NEWS

Europe Considers New Cybercrime Agency

The Council of the European Union recently requested that a feasibility study be conducted to determine the potential effectiveness of a new agency to coordinate international cybercrime investigations. This proposed agency would work to ensure that member countries of the Council of Europe's Cybercrime Convention would have 24-hour-a-day access to a contact that would assist in cybercrime investigations. An additional mission of the new agency would be to provide evidence of the need for more countries to ratify the Council of Europe's Cybercrime Convention, which requires standardized laws for certain cybercrime behaviors. Further, the agency would potentially be responsible for collecting data on cybercrime throughout Europe, and potentially throughout other member countries, compiling this data and preparing reports that would potentially aid in the development of new laws and policies related to regulation of cybercrime. The timeline for the development and implementation of this agency is yet undetermined, as the feasibility study is expected to address questions on where the agency should be housed, how the agency should be financed, and the scope of the agency's duties.

Source: Kirk, J. (2010, April 29). Europe Considers New Cybercrime Agency, *San Francisco Gate Chronicle*. Retrieved from: www.networkworld.com/news/2010/042910-europe-considers-new-cybercrime.html?source=nww_rss.

Review Questions

1. What is meant by the term *high technology*? What is high-technology crime?

2. In discussing high-technology crime, what is meant by the term *computer*?

3. Is the high-technology crime problem serious enough to begin reevaluating the way in which the criminal justice field handles such investigations? Why do you feel this way?

4. Historically, what was the difference between a computer crime and a cybercrime? Is there a need to continue differentiating between the two?

5. Why do you think hacking was historically viewed as the most common high-technology crime? What crime do you think could possibly replace hacking as the most commonly occurring high-technology crime?

6. It has been stated that digital piracy is not investigated as often as other high-technology crimes. Do you feel that digital piracy is a crime that more law enforcement agencies should be investigating?

7. What, if any, problems would you foresee if law enforcement agencies were to investigate more criminal cases involving digital piracy or auction fraud?

8. Do you feel that it would be important for more law enforcement personnel to receive training on how to locate, seize, and store electronic evidence? How could such knowledge assist law enforcement personnel who do not investigate high-technology crimes?

9. Do you feel that evidence of high-technology crimes should be handled differently from other forms of evidence in terms of its admissibility in the criminal trial process? Why or why not?

10. Which of the crimes overviewed in this chapter do you believe warrants the most consideration? Why this particular crime?

Online Resources

The Computer Emergency Response Team—Provides information related to the frequency and types of attacks against personal computers. Available at www.cert.org.

High Technology Crime Investigators Association—Professional association designed to provide training and information for individuals who investigate high-technology crimes. Available at www.htcia.org.

Internet Crime Complaint Center—Partnership between the National White Collar Crime Center, Bureau of Justice Assistance, and the Federal Bureau of Investigation that provides a means of reporting Internet-based crimes and maintains reports on the frequency of many online criminal activities that are reported. Available at www.ic3.gov.

Chapter 2

Hackers, Crackers, and Phone Phreaks

In the past when the term *hacker* was first mentioned it was not uncommon for people to conjure up an image of a small, fragile, nerdy-looking teenager sitting in front of his computer, playing video games. Today it can be said that not only would such an appraisal of hackers be inappropriate, it would be troubling and incorrect for people to believe that only teenagers and children are engaging in hacking-related behaviors. The truth is that there are many adults who engage in hacking on a day-to-day basis, and many times these older perpetrators commit very malicious acts involving computers and networks. So why did people historically conjure up the image of the teenager? There are several possible reasons that would explain such an initial response. First, when computers were originally released, it may have seemed to some that the devices were reserved for teenagers or those who were among the intellectually elite, a scenario that would explain the nerd-like image of the hacker. Additionally, many teenagers did devote countless hours to learning how to operate computers when they were first released. Several of these individuals foresaw the potential role that computers could play in the future of society. With this in mind, many teenagers were intent upon learning more about computers as a means of ensuring that they would have a secure job when computers eventually began to catch on with businesses and corporations. For others, playing with the technology provided an opportunity for young people to challenge themselves while having fun.

The addiction that some of these individuals maintained for their computers was certainly a factor in the development of any aforementioned misconceptions. The truth, however, is that Hollywood most likely played almost as important a role in ingraining the image. There was a point at which Hollywood began releasing films that provided images of a teenager using his or her computer to wreak havoc on America; often the level of mischief was so great that the safety of Americans was threatened. Sadly, if individuals are not informed and trained in regard to understanding the term *hacker*, then they will assume that the individuals in such

DOI: 10.1016/B978-1-4377-5582-4.00002-9

movies—perhaps most notably *Hackers* and *WarGames*—are representative of the entire hacker population. Of course, there may be individuals who fit this image, but it is generally accepted that the image is nowhere near representative of the entire population.

The Evolution of the Term *Hacker*

Understanding of the term *hacker* is further complicated because there are many definitions available for the term. Perhaps the best method of understanding the connotations related to the term is to briefly examine the term's history and development. The definition for the term *hacker* has undergone many dramatic changes since its inception. Today, individuals who claim to be hackers argue that true hackers are interested in furthering computer security and that those who do not conform to this belief system are not hackers in the truest sense of the word. It is these individuals who do not care to aid in improving computer security that are benefiting, albeit occasionally in a negative sense, from the aforementioned emphasis in Hollywood and media reports.

The origin of the term can be traced back to the Massachusetts Institute of Technology (MIT), which was one of the first institutions in the United States to offer computer programming and computer science courses. The term is believed to have first been used in a computer context by the members of the Artificial Intelligence Lab at MIT. These individuals were not criminals. In fact, according to Steven Levy, who has written extensively on the history of hacking, they were a highly devoted research team. This is not to say that these individuals did not violate the rules of the university. Many of the team members were reportedly in constant violation of university rules and procedures concerning the number of hours a computer could be used by a student or faculty member. The members began referring to themselves as hackers because they were able to take computer programs and make them perform actions not originally intended by the designers of the computer software. The term is believed to have developed as a practical joke and a feeling of excitement because the team members would "hack away" at the keyboards for hours at a time.

Prior to the use of the term by the Artificial Intelligence Lab members, Levy claims that the term *hack* was used by other MIT students to refer to any practical joke that was imbued with creativity, extreme style, originality, or technical virtue. The term originated on the MIT campus in the early 1950s, and it is commonly held to this day that many, if not all, students will eventually perform a hack before graduating from the university. The catch is that the hacks must not only be high-profile and original but must also be committed anonymously. It could be considered a rite of passage for MIT students. Readers who are interested in learning more about these

creative practical jokes and hacks are encouraged to visit the MIT website, where one can order a variety of official publications concerning the history of successful hacks at the university.

The term *hacker* remained a relatively obscure term until crimes committed via computer began gaining more publicity in the media. It was at this time that the term became associated with individuals who were using their personal computers to gain unauthorized access to other individuals' and businesses' computers. Dorothy Denning, a well-known researcher and computer scientist who has studied hackers since the early 1990s, states that the original members of the MIT Artificial Intelligence Lab immediately made known their discontent with the use of the word in relation to such negative and criminal activities. The term *cracker*, a combination of hacker and criminal, was recommended as a possible term to describe the individuals who were misusing computers. This term, however, was not as accepted during the early years of media coverage, and with the release of the aforementioned films and now numerous texts on hacking, the term *hacker* has become even further ingrained into the vocabulary of society. It would be extremely difficult, perhaps even impossible, to completely distinguish the two terms today.

This is not to say that the term *cracker* is not utilized by individuals who deal with high-technology crime. *Cracker* is a recognized term today; but returning to Eoghan Casey's definition, the term is generally used to refer to one who violates software copyright protections and gains inappropriate access to password-protected files and services. The issue of copyright protection has become an extremely hot topic in recent years with the advent of peer-to-peer networking and the sharing of music and video files via the Internet. Within the computer science community, and more specifically within the hacking community, the difference between hacking and cracking is still recognized today. Outside of these communities, however, the two terms have come to mean almost the same thing. If the terms arise in conversation, it is important to examine the context in which the term is used. It is possible that the user is intending to talk about one form of computer specialist and may accidentally refer to the other form of computer specialist—thereby misusing the terminology. In addition, some individuals most likely do not realize that there is a difference between the two and therefore cannot make an attempt to apply the terms properly.

The Introduction of Hacking to the Public

Threats associated with computer crime existed long before technology evolved to a point where two or more computers could connect and share information and resources. It was, however, this initial connecting of computers that has ultimately led to computers becoming an instrument

of mass harm and nuisance. The linking of computers to share resources has raised the level of potential harm to the point at which computer-related attacks can impact national, as well as international, security. The original reason for connecting computers was to share files and computing power, with the foundation for this principle beginning with the development of the ARPANET (Advanced Research Projects Agency Network). The ARPANET was developed when four sites around the United States were linked together as a means of sharing information and resources. In this respect, the ARPANET could be considered the forerunner of the Internet, although it should be noted that there have been several additional developments in computer technology that have led to the current state of networking and the current version of what we now refer to as the Internet. The original launching of the ARPANET was heralded as a new advancement in information sharing and a tool that would impact research for generations. Some believed that the ARPANET would change the way of life for most individuals. It could be considered ironic that technology developed as a means of improving research, education, training, and information sharing has developed into one of the most commonly used tools by criminals in history.

The potential dangers of computing were not immediately apparent to these and other researchers. Several years later a number of high-profile media events introduced the general public to the potential dangers of computer hacking. These events began in early 1983 with a series of rather serious computer break-ins. During the course of investigating them, it was discovered that at least 60 computers belonging to the Memorial Sloan-Kettering Cancer Center and the Los Alamos National Laboratory were compromised. The news media became interested in the case, and before long the Federal Bureau of Investigation (FBI) was brought into the investigation. As a result of the FBI's investigation, it was determined that the break-ins were committed by a gang of teenagers that referred to themselves as the "414 Gang"—likely a tribute to the area code in which they lived. The public immediately began demanding better protection from this new generation of high-tech youths. Interestingly enough, the public seemed to automatically associate the offenders' ages with the fact that the crimes involved the use of computers. This misconception was perhaps further reinforced when other media outlets began covering the crimes and discussed the young age of the individuals involved in the acts.

Following the events surrounding the Los Alamos Research Facility, and several additional incidents involving computers, Congress began work on legislation that would curtail the incidence of computer-assisted crime. In 1986, legislation was finally approved and termed the Computer Fraud and Abuse Act (CFAA). The CFAA made the unauthorized access of a federal interest computer an illegal act. While the CFAA was designed with the best of intentions, the truth is that the legislation only addressed

hacking into federally controlled computers, unless the incident occurred across two or more different states. Computers owned or controlled by state governments and other non-federal entities were generally not addressed, leaving several states to follow the suggestion of the federal government and implement similar legislation concerning the misuse of computer technology in criminal activity.

Only a couple of years after the passing of the CFAA, the public was once again introduced to a high-profile crime involving the intersection of computers and technology. On November 2, 1988, Robert Morris, a Cornell University graduate student, inadvertently released a computer program that would come to be referred to as a *worm* program.[1] Morris was working on a graduate degree in computer science with an emphasis in computer security. The program he wrote was allegedly a practice program that he intended to use as a test and then remove from the systems he infected. The program was to be installed on a computer within the MIT computer lab. Once installed on the first computer, the program would copy itself onto the other computers in the lab and then remain hidden until Morris could remove it from the system. Unfortunately, due to an error in coding, the program began replicating itself at unforeseen speeds. By taking advantage of a security defect in the network, the program was able to copy itself onto between 2,000 and 3,000 computers, resulting in the computers being forced to shut down after they ran out of memory and processing capacity. The companies affected by the virus were believed to have spent thousands of dollars in time and wages to repair the damage caused by the software program.

On November 7, 1988, the FBI became involved with the case. Many speculate as to whether Morris would have ever been discovered had he not contacted authorities to inform them that it was an accident and that he was sorry. Once Morris was located, the problem arose of how to press charges. On the basis of information provided during the investigation, there was no legal statute under which to charge Morris. Eventually, it was determined that the Computer Fraud and Abuse Act of 1986 could possibly be used to prosecute Morris. The results of Morris being charged under the CFAA were interesting. Officially, this was the first time an individual had been charged under the newly enacted legislation, and there was still debate as to whether the charges were properly filed. Because of these facts, Morris gained extreme notoriety for being the first person charged under the CFAA, leading to Morris being inducted into several "hacker halls of fame." It is undetermined whether Morris would have received these honors had he not been the first to be prosecuted under

---

[1] A worm is a computer program that, unlike a virus, is not usually written as an attempt to damage a computer system. Instead, a worm program will usually replicate itself repeatedly and then resend itself back out over the Internet. This constant duplication and re-mailing can slow down a network to the point of collapse, as was the case of Robert Morris's worm program.

the new computer crime statutes. Morris is not referenced much beyond his prosecution and inadvertent discovery of the worm program, despite the fact that he is now an associate professor at MIT and has done remarkable work in the field of computer science.

Because of the unique circumstances surrounding the case of Robert Morris, the Cornell Commission was developed and charged with the dual task of investigating the incident and making recommendations on how to prevent future occurrences. It was the opinion of the Commission that Morris's actions were indeed accidental in nature, and that several security deficiencies in the computer systems were detected as a result of his actions. It was this detection of security defects that led to the Commission's indication that the worm program resulted in a positive change and improvement in computer security. The Computer Fraud and Abuse Act required that the prosecution prove that Morris "intentionally and without authorization accessed federal interest computers." The Commission determined that during the course of the trial the prosecution did in fact prove that Morris's actions were intentional because he released the worm into the computer lab with premeditation; this belief was based on testimony that indicated Morris took advantage of several holes in the UNIX operating system during the process of implanting the worm program. Despite the fact that Morris had not intended for his program to be let loose upon the world, he was still convicted on January 22, 1990, and on the recommendation of the Cornell Commission it was determined that Morris's punishment should not be reduced. Morris was ultimately sentenced to three years probation, fined $10,000, and ordered to perform 400 hours of community service.

The cases involving the 414 Gang and Robert Morris initiated the process of highlighting hacking in the media. However, the two crimes involved only limited media coverage when they occurred. The 414 Gang had brought attention to the citizens of Minnesota and the surrounding states, but overall the majority of the nation remained unaware of the problem. Over the next few years the entire nation would slowly become aware of the possible power a hacker could possess, as well as the publicity such acts could generate.

During the late 1980s and the early 1990s, individuals around the world were introduced to the escapades of a young man named Kevin Mitnick. As a teenager in the 1980s, Mitnick was constantly in trouble with authorities because of his inappropriate activities involving computers. In the early 1990s, however, Mitnick's name became very well known when he was tracked cross-country by a computer engineer whose computer he had illegally accessed. Mitnick witnessed the engineer in question on television discussing a new technique for converting a cellular phone into a digital receiver. Wanting the information for himself, Mitnick hacked into the engineer's computer and took the plans associated with the technique. The engineer, upon discovering that his