Chapter 1
An Introduction to High-Technology Crime

Chapter Outline

I. Introduction
II. What is High-Technology Crime?
- A. High-technology crime refers to any crime involving the use of high-technology devices in its commission.
  - 1. High-technology devices include computers, telephones, check-reading machines, credit card machines.
  - 2. High-technology crimes can range from traditional crimes committed prior to technological advances to newer crimes that rely on high-technology devices for a crime to be committed.
  - 3. The two best known classifications of high-technology crimes are computer crimes and cybercrimes.
- B. Computer Crimes
  - 1. Casey has traditionally defined computer crime as criminal activities involving a computer that are made illegal through statute.
  - 2. Computer crimes involve the use of computers in the following ways:
    - a. Computer as an instrument of the crime.
      - i. Crime cannot be committed with the use of the computer to commit the act.
    - b. Computer as the focus of a crime.
      - i. Computer is the intended target of the criminal.
    - c. Computer as a repository of evidence.
      - i. Criminal will store evidence on the computer.
  - 3. Hacking is the most famous and commonly read about computer crime.
    - a. Hacking refers to the unauthorized access of another person's computer.
    - b. Hacking involves the use of a computer as an instrument of the crime.
    - c. The computers used in hacking will probably maintain some form(s) of evidence that could be used to confirm the identity of the hackers.
- C. Cybercrime
  - 1. According to Casey, cybercrime refers to any crime that involves a computer and a network, in which a computer may or may not have played an instrumental part in the commission of the crime.
  - 2. Identity theft is an example of a cybercrime.
    - a. Identity theft involves the theft of someone's personal information such as their credit card number or social security number.
    - b. There are several methods used by criminals to obtain personal information, which may or may not involve the use of a computer or a network to commit the crime.
  - 3. Some consider computer crime to be a subdivision of cybercrime that warrants its own definition and understanding.
  - 4. The determining factor between computer crimes and cybercrimes is whether a statute is present to criminalize the use of the computer in the criminal act.

D. Consolidating High-Technology Crimes
    1. A strong argument could be made that distinction between a computer crime or a cybercrime is nothing more than a trivial distinction.
    2. The definition of a computer crime is now beginning to blur into the definition of a cybercrime.
        a. This is because the Internet is now being used in many criminal activities that rely on computer technology.
    3. The author refers to the term "high-technology crime" to criminal activities that may have at one time been considered either a computer crime or a cybercrime.

III. How Serious is the High-Technology Crime Problem?

A. High-technology crimes include:
    1. Hacking
    2. Digital Child Pornography
    3. Identity Theft
    4. Intellectual Property Theft
    5. Online Fraud
B. The rate of high-technology crimes has steadily increased in recent years.
C. Crime is not isolated to the United States.
D. 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.
    1. Jurisdictional issues is one of the problems associated with high-technology crimes.
        a. Very difficult to determine who has authority to investigate these crimes.
        b. A person can live in one country, but the crime is committed in another country.
E. According to the Internet Crime Complaint Center, complaints of fraud and attempted network intrusions were up 33.1% for the year 2009 compared to 2007.
F. Some companies have hired individuals whose sole job is to do nothing more than write anti-virus software programs or defend the computer network against outside hackers.
G. Digital child pornography, online fraud, and identity theft crimes have increased over the years.
H. According to Equifax, identity theft has affected more than 27 million Americans in recent years.
    1. Identity theft is perhaps such an attractive crime because it is possible to commit the crime and move on before the victim even realizes they have been victimized.
I. The frequency of high-technology crime has created a problem for law enforcement personnel because of the need for training and equipment.
    1. Recognition and response to these crimes is better today than it was 10 years ago.
    2. Today, budget shortfalls can impede the investigation of high-technology crimes.

a. This is especially true in smaller, rural police and sheriff's departments.
b. Criminals may retreat to these smaller communities in hopes of not getting caught.

IV. The Purpose of This Work

A. Provide a starting point for investigators, students, and private citizens who are to come into contact with these crimes in the near future.
B. 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.
C. Chapter Outline

1. The Criminal Acts

a. Chapters 2–7 will focus on the most commonly encountered high-technology crimes.
b. Each chapter discusses the physical-world techniques involved in committing the criminal act.
c. Chapter 2—Hacking and Phreaking

i. Investing hacking 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 criminal activity.
ii. Phreaking refers to the theft of telecommunication services.
iii. Historically hackers would also be considered a phone phreak because one activity complements the other and assists in ensuring that the hacker remains unidentified.
iv. Chapter contains a brief history of hacking and phreaking, a discussion of the different types of hackers, and the tools and techniques used by hackers, and finally, the hacker/phreaker subculture will be introduced.

d. Chapter 3—Identity Theft

i. Identity theft involves the theft of another's personal identity, credit identity, or physical identity.
ii. Considered to be the fastest-growing high-technology crime.
iii. One of the few high-technology crimes that originated without the use of advanced technology and still occurs more frequently as a result of old-fashioned con artistry rather than advanced technological skills.
iv. This chapter discusses the evolution of physical identity theft, how the Internet and technology have affected identity theft, how identity theft is accomplished, how this crime is committed, and information about identity theft in the future.

e. Chapter 4—Digital Child Pornography

i. Child pornography is regarded by many as the most physically damaging of the high-technology crimes.
ii. Prior to the public release of the Internet, child pornography had begun to decline.

iii. Child pornography is one of the most investigated high-technology crimes.
iv. There has been growing arguments regarding the illegality of child pornography that is manufactured in a country where such materials are legal.
v. 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.
vi. This chapter gives a brief history of child pornography and children's rights, what child pornography is used for, the effects of digitization and the Internet on child pornography, and how this crime is committed today, and will conclude with a discussion of statutes and court decisions concerning investigating child pornography.

d. Chapter 5—Internet Fraud
i. This chapter contains an overview of how the Internet has become a haven for fraudulent behavior in the twenty-first century.
ii. Internet fraud includes online auction fraud, adoption fraud, purchasing wives online, online prostitution, and the Nigerian 419 scam.
iii. Each crime will be discussed as well as how the crimes are committed and what can be done to prevent the crimes.

e. Chapter 6—Online Harassment and Cyberstalking
i. Harassment and bullying have been topics of concern for educators and child care experts for years.
ii. There has been a growing number of cases involving harassment via the Internet.
iii. Social networking websites are discussed, as well as how they can be used by harassers and bullies.
iv. Cyberstalking may become much more serious and dangerous than online harassment should the stalking behaviors move from the Internet to the physical world.
v. Cyberstalking has been criminalized in many states only within the last few years, and some states do not address the activity as a crime.
vi. This chapter discusses how cyberstalking occurs and why law enforcement personnel should take it seriously.

f. Chapter 7—Intellectual Property Theft
i. In this chapter, the crimes of digital file-sharing and digital piracy are discussed.
ii. Thanks in part to the increasing sizes of computer storage media and improving file compression software, it is now possible to store hundreds of movies or hundreds of thousands of songs, which can be traded via the Internet or traditional methods.
iii. This crime is not investigated by law enforcement personnel as often as other types.

2. Investigating High-Technology Crimes
    a. The focus of this section is on providing information relating to the actual investigation of high-technology crimes.
    b. Chapter 8—Investigating Crime Online
        i. Introduces readers to online sting operations.
        ii. Also focuses on legal issues associated with online sting operations, especially online entrapment.
    c. Chapter 9—Search Warrants for Digital Evidence
        i. This chapter focuses on the specificity of search warrants when dealing with the seizure of digital evidence.
        ii. Information on drafting a search warrant, establishing the search warrant execution team, and preplanning for the execution of the warrant are discussed.
        iii. A brief look at warrantless searches and digital evidence seizure is presented.
    d. Chapter 10—Executing the Search Warrant
        i. This chapter provides a step-by-step guide for executing a search warrant involving a computer or other high-technology device.
        ii. This chapter also includes a discussion of how to protect the integrity of the evidence for instance in which the case goes to trial.
3. Introduction to Computer Forensics and the Future of Technology Crime
    a. The third section of the book introduces the reader to networking and computer forensics.
    b. This section contains 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.
    c. Chapter 11—An Introduction to Computer Forensics and Software
        i. This chapter introduces readers to the field of computer forensics, with specific coverage of how the field has developed over the last several years, and information on some of the more commonly used software packages.
        ii. Legal issues associated with the capture and admission of digital evidence are discussed.
        iii. Readers learn how adherence to the computer forensics process can result in the proper admission of evidence during a criminal trial.
    b. Chapter 12—Emerging Issues in the Investigation of High-Technology Crime
        i. The issue of cyberterrorism is discussed in this chapter.
        ii. Readers are exposed to some of the more recent studies on cyberterrorism, what is meant by the term “cyberterrorism,” and what techniques may be utilized by terrorists in the future.
        iii. Chapter concludes with an examination of the role international law currently plays in the investigation and

prosecution of high-technology crimes today.

c. Chapter 13—The Development and Role of Cybercriminology
   i. In this chapter, the reader is provided with an introduction to the emerging field of cybercriminology.
   ii. It also includes a discussion of the role of the younger generation in fighting high-technology crime.
   iii. This chapter introduces readers 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.

Key Terms

Computer: An electronic device that allows the user to input information, process that information, and then receive results that are based upon the information provided by the user.

Computer Crime: Criminal activities involving a computer that are made illegal through statute.

Computer Forensics: The process of applying science and computers to the investigation of criminal acts.

Cybercrime: 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.

Cybercriminology: The study of why people engage in high-technology crimes.

Digital Evidence: The term used to describe evidence stored on a computer or other magnetic storage media.

Hacking: The unlawful access of another's computer without the legitimate owner's permission.

High Technology: Highly developed electronic devices.

High-Technology Crime: Any crime involving the use of high-technology devices in its commission.

Identity Theft: The theft of someone's personal information such as their credit card number or social security number.

Phreaking: The theft of telecommunication services.

Technology: Mechanical or electrical devices that assist individuals in their day-to-day activities.