Chapter 15

Technology and Crime It's a Double-Edged Sword

Audio

Listen to the Audio

Listen to audio

Golden-i/Rex Features/AP Images

Learning Objectives

15.1 How does advancing technology produce new forms of crime?

15.2 How does high technology provide new criminal opportunities?

15.3 What is the extent of cybercrime today?

15.4 Name some of the federal laws targeting

15.3 What is the extent of cybercrime today?

15.4 Name some of the federal laws targeting cybercriminals.

15.5 Describe the characteristics of cybercriminals.

15.6 What new technologies are being used in today's fight against crime?

15.7 What is being done today to combat cybercrime and to secure the Internet?

15.8 What are some of the personal freedoms that are threatened by today's need for advanced security?

Introduction

Politics has long provided plenty of fodder for news organizations, and social media participants often find themselves viewing or contributing to discussions of political positions on the Web. So, it should have come as no surprise when, in 2017, government watchdogs identified attempts that had been made by Russia and other countries to influence the U.S. presidential election one year earlier. Following that discovery, the Senate Select Committee on Intelligence, along with the House Permanent Select Committee on Intelligence, began separate probes on claims that Russian hacking may have influenced the election.[1685] One year later, the U.S. Department of Justice charged nine Iranians with a massive cyber theft campaign that had been conducted on behalf of that country's Islamic Revolutionary Guards. Not all of the crimes perpetrated on the Internet are carried out by state-actors, of course.[1686] This chapter discusses technology and crime, and it is clear that the number of crimes

Technology and Crime

15.1 How does advancing technology produce new forms of crime?

Audio

Listen to the Audio

Listen to audio

Watch

Advancing Technology and Crime

Technology and crime have always been closely linked. The con artist who uses a telephone in a financial scam, the robber who uses a firearm and drives a getaway car, even the murderer who wields a knife—all employ at least rudimentary forms of technology in the crimes they commit. Technology can be employed by both crime fighters and lawbreakers. Early forms of technology, including the telegraph, telephone, and automobile, were embraced by agents of law enforcement as soon as they became available. Evidence derived from fingerprint and ballistics analysis is routinely employed by prosecutors; and

analysis is routinely employed by prosecutors; and emerging technologies promise to keep criminologists and law enforcement agents in step with high-tech offenders.

As technology advances, it facilitates new forms of behavior, so we can be certain that tomorrow's crimes will differ from those of today. Personal crimes of violence and traditional property crimes will continue to occur, but advancing technology will create new and as-yet-unimaginable opportunities for criminals and other international actors positioned to take advantage of it and of the power it will afford.

The Kremlin in Moscow, Russia. In 2019 the U.S. Congress investigated Russian activities that had been intended to influence U.S. elections in 2016 and 2018. How are technology and crime related?
Alexander Tolstykh/Shutterstock

A frightening and early preview of such possibilities was seen during the collapse of the Soviet Union when the resulting social disorganization made the acquisition of fissionable materials, stolen from Soviet stockpiles, simple for even relatively small outlaw organizations. In what is a nightmare for authorities

organizations. In what is a nightmare for authorities throughout the world, Middle Eastern terrorist groups are still making efforts to acquire former Soviet nuclear weapons and the raw materials necessary to manufacture their own bombs, and some evidence suggests that nuclear weapons parts may have already been sold to wealthy international drug cartels and organized criminal groups, who could hoard them to use as bargaining chips against possible government prosecution.

About five years ago, the White House identified the Chinese military as the source of cyberintrusions into public and private Web sites throughout the United States; and in 2014, a federal grand jury returned indictments charging five Chinese military officers with economic espionage and conspiracy to hack into computers located in the United States. Federal prosecutors said that the men had stolen trade secrets and other sensitive business information.[1687] Since that time, other large American companies, including Yahoo! corporation, Bank of America, J.P. Morgan, and Sony Pictures, have been the victim of similar attacks by other parties. In 2018, the U.S. Department of Justice obtained a conviction in U.S. federal court against a China-based manufacturer and exporter of wind turbines, Sinovel Wind Group Co., Ltd., that conspired with others to steal trade secrets from a U.S.-based company.

U.S. companies are not the sole victims of cyberattacks, of course, and in a 2017 example, Ruslan Stoyanov, a key cybercrime investigator at Russia's biggest cybersecurity firm, Kaspersky Labs, was arrested in his home country and charged with treason. Stoyanov was

cybersecurity firm, Kaspersky Labs, was arrested in his home country and charged with treason. Stoyanov was taken into custody along with a senior Russian FSB intelligence officer, Sergei Mikhailov, who also faced treason charges. Mikhailov was the deputy head of the information security department of the Russian national security service (FSB). Both men were accused of taking bribes from foreign entities to facilitate computer intrusions in various places around the world.[1688]

High Technology and Criminal Opportunity

15.2 How does high technology provide new criminal opportunities?

Audio

Listen to the Audio

Listen to audio

The twenty-first century has been termed the postindustrial information age. Information is vital to the success of any endeavor, and certain forms of information hold nearly incalculable value for those who possess it. Patents on new products, pharmaceutical formulations, corporate strategies, and the financial resources of corporations all represent competitive and corporate trade secrets. Government databases, if infiltrated, can offer terrorists easy paths to destruction and mayhem.

Some criminal perpetrators intend simply to destroy or alter data without otherwise accessing or copying the information. Disgruntled employees, mischievous computer **hackers**, business competitors, and others may have varied degrees of interest in destroying the records or computer capabilities of others.

High-tech criminals seeking illegitimate access to computerized information take a number of routes. One is the path of direct access, wherein office workers or corporate spies, planted as seemingly innocuous employees, use otherwise legitimate work-related entry

employees, use otherwise legitimate work-related entry to a company's computer resources to acquire wanted information.

Another path of illegal access, called *computer trespass*, involves remote access to targeted machines. Anyone equipped with a computer and Internet access has potential access to numerous computer systems. Many such systems have few, if any, security procedures in place. Similarly, electromagnetic field (EMF) decoders can scan radio frequency emanations generated by all types of computers. Keystroke activity, internal chip-processed computations, and disk reads, for example, can be detected and interpreted at a distance by such sophisticated devices. Computers secured against such passively invasive practices are rarely found in the commercial marketplace, although the military had adopted them for many applications. Within the last decade, wireless networking has heightened fears of data theft, and cell phones, handheld devices, and other forms of radio communication offer opportunities for data interception.

The realities of today's digital world have led to a form of crime called cybercrime, and to new laws intended to combat it. Simply put, **cybercrime**, or *computer crime*, is any violation of a federal or state **computer-crime** statute. Many argue that only those crimes that use computer technology as central to their commission may properly be called "cybercrimes." However, a number of other kinds of offenses can also be described as cybercrimes. A Federal Bureau of Investigation (FBI) typology distinguishes between five types of cybercrimes: (1) internal cybercrimes, such as

types of cybercrimes: (1) internal cybercrimes, such as viruses; (2) Internet and telecommunications crimes, including illegal hacking; (3) support of criminal enterprises, such as databases supporting drug distribution; (4) computer-manipulation crimes, such as embezzlement; and (5) hardware, software, and information theft.[1689] **Table 15-1** lists these five categories, with additional examples of each. A somewhat different typology was developed by the U.S. Department of Justice and published in the 2018 report of the Attorney General's Cyber Digital Task Force. That report can be accessed at **https://www.justicestudies.com/pubs/cybertaskforce.pdf**.

Check Your Understanding

Table 15-1: Categories of Cybercrime

When discussing cybercrime, it is important to realize that a huge number of today's financial transactions are computerized. Although most people probably think of money as bills and coins, money today is really just information—information stored in a computer network, possibly located within the physical confines of a bank, but more likely existing as bits and bytes of data on service providers' machines. Typical financial

of a bank, but more likely existing as bits and bytes of data on service providers' machines. Typical financial customers give little thought to the fact that very little "real" money is held by their bank, brokerage house, mutual fund, or commodities dealer. Nor do they often consider the threats to their financial well-being by activities such as electronic theft or the sabotage of existing accounts. Unfortunately, however, the threat is very real. Computer criminals equipped with enough information (or able to find the data they need) can quickly and easily locate, steal, and send vast amounts of money anywhere in the world.

No reliable estimates exist as to the losses suffered in such transactions due to the activities of technologically adept criminal perpetrators. Accurate estimates are lacking largely because sophisticated high-tech thieves are so effective at eluding apprehension.

Survey

The Seriousness of Cybercrime

The Extent of Cybercrime

15.3 What is the extent of cybercrime today?

Audio

Listen to the Audio

Listen to audio

A recent CSO (Chief Security Officer) Cyber Security Watch Survey, a cooperative effort between the U.S. Secret Service, Deloitte & Touche, Carnegie Mellon's Software Engineering Institute (CERT), and *CSO* magazine, found that a sophisticated cybercrime-fueled underground economy exists in America and that its members continue to develop a high-level arsenal of damaging software tools with which most companies cannot keep pace while remaining focused on their core businesses. One recent global report on the cost of cybercrime found the following:

1. Cybercrimes continue to be on the rise and so do the costs associated with them.

2. The most costly cybercrimes are those caused by malicious insiders.

3. Business disruption represents the highest cost, followed by the costs associated with information loss. [1690]

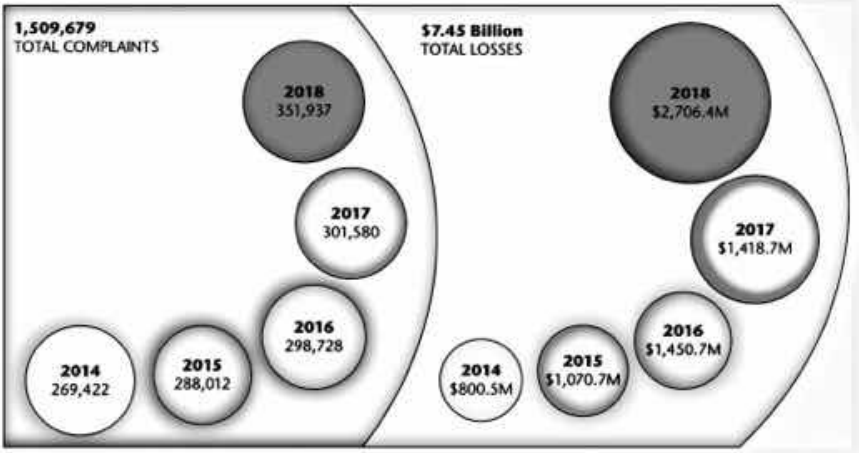
Dr. Ali-Reza Ghasemi and his wife, Shahla Ghasemi, of Tampa (Florida). They lost $400,000 to an advance fee scheme on the Internet. Advance fee schemes (often called Nigerian e-mail fraud because many of the messages appear to come from Nigeria) promise victims a lot of money in return for advancing fees to cover legal services and transfer of funds. How can you tell when an e-mail message is likely to be a fraud?
William S. Speer/Bloomberg/Getty Images

Another industry group, the Ponemon Institute, in conjunction with IBM, surveyed 477 business organizations in 13 countries in 2018 and found that the typical company lost $3.86 million in each cyberattack. The average cost for each lost or stolen record containing sensitive and confidential information was put at $148.[1691] **Software piracy**, or the unauthorized and illegal copying of software, is also rampant. According to the Business Software Alliance, global losses from pirated software (known as *warez* in the computer underground) totaled over $70 billion in 2017.[1692] One out of five pieces of installed software in the United States was unlicensed in 2018. Finally, **Figure 15–1** shows five-year totals of cybercrime-related incidents reported to the Internet Crime Complaint Center (IC3), along with estimated cumulative losses to corporations and individuals during that time frame. The IC3, which is operated by the FBI, accepts online Internet crime complaints from either the victim or from a third party to the

complainant. It can be reached online at **https://www.ic3.gov**.

Figure 15-1

Cybercrime-Related Criminal Complaints and Estimated Financial Loss, 2014–2018



Sources: FBI, Internet Crime Complaint Center (IC3).

Phishing (pronounced "fishing") is a relatively new scam that uses official-looking e-mail to steal valuable information such as credit card numbers, Social Security numbers, user IDs, and passwords from victims. The e-mails appear to come from a user's bank, credit card company, retail store, or Internet service provider (ISP) and generally inform the recipients that some vital information in their account urgently needs to be updated. Those who respond are provided with an official-looking Web form on which they can enter their private financial information. Once the information is submitted, it enters the phisher's database.

The Anti-Phishing Working Group (APWG), a coalition of banks and ISPs, says that a typical phishing scheme reaches up to 1 million e-mail in-boxes. The watchdog group has identified more than 277,000 different phishing Web sites.[1693] Although servers that run those

phishing Web sites.[1693] Although servers that run those sites can be anywhere in the world, the APGW found that 46% of them are located in the United States.

Phishing sites often attempt to hijack brand names, and some phishers are capable of sending e-mails that are difficult to distinguish from legitimate ones. When that happens and customers respond to those e-mails in significant numbers, a brand (such as the name of a bank or credit card company) is said to have been hijacked. Some observers have noted that in addition to losses suffered by individuals and institutions, phishing has the potential to threaten the viability of e-commerce and to call into question the safety of all Web-based financial transactions.[1694]

Check Your Understanding: Phishing

Select each of the rows below to learn more about phishing.

How does phishing work?

Reveal Answer ⌄

What are spear phishing and whaling?

Reveal Answer ⌄

Cybercrime for Criminal Mischief

Audio

Listen to the Audio

Listen to audio

Not all cybercrime is committed for financial gain. Some types of computer crime, including the creation and transmission of destructive computer viruses, "worms," spyware, and other malicious forms of programming code (often called *malware*), might better be classified as "criminal mischief." Perhaps not surprisingly, these types of activities are typically associated with young, technologically sophisticated male miscreants seeking a kind of clandestine recognition from their computer-savvy peers. Computer crimes committed by youthful and idealistic offenders may represent a novel form of juvenile delinquency—one aimed at expressing dissatisfaction with the status quo.

Computer viruses have shown signs of becoming effective terrorist-like tools in the hands of young, disaffected "technonerds" intent on attacking or destroying existing social institutions. A **computer virus** is a computer program that is designed to secretly invade computer systems to modify the way in which they operate or to alter the information they store.[1695] Other types of destructive programs are logic bombs, ransomware worms, and Trojan horse routines. Distinctions among these programs are based on the way in which they infect targeted machines or on the way in which they behave once they have found their

way in which they behave once they have found their way into a computer. Not all malware is created by disaffected programmers. Recently, computer security company Symantec announced the discovery of what it called the "world's most sophisticated computer malware."[1696] The software code, named Reign, is a highly sophisticated worm designed to provide backdoor access to computers that it infects. It is virtually undetectable and can modify its own code or simply disappear from infected systems in order to avoid discovery. Cybersecurity experts suspect that it was developed by a Western intelligence agency to target foreign governments and that it may have been in operation for years before its discovery. Reign follows in the footsteps of Stuxnet, a hacking software that was apparently created by Western governments in 2010 to disrupt Iranian computers in that country's nuclear facilities. Similarly, a few years ago, a stealth e-mail virus called *WannaCry* made headlines when it disabled millions of computers around the world. WannaCry fell into the category of "**ransomware**", and its creators demanded payments in Bitcoins to "free" affected machines, and to allow their users to access important data that the ransomware had effectively encrypted. While some experts claimed that the ransomware attacks originated in North Korea, others said that they used software exploits developed by the National Security Agency—which, although highly classified, had been exposed by the hacker group known as Shadow Brokers. Another ransomware program called Adylkuzz, began infecting computers shortly after the *WannaCry* outbreak had been contained. **Figure 15–2** diagrams the anatomy of a ransomware attack.

Cybercrime and the Law

15.4 Name some federal laws targeting cybercriminals.

Audio

Listen to the Audio

Listen to audio

In the early years of computer-based information systems, most U.S. jurisdictions tried to prosecute unauthorized computer access under preexisting property crime statutes, including burglary and larceny laws. Unfortunately, because the actual carrying off of a computer is quite different from copying or altering some of the information it contains, juries were confused by how such laws apply to high-tech crimes and computer criminals were often let free. As a result, all states and the federal government developed computer-crime statutes specifically applicable to invasive activities that illegally access stored information. One of the first such laws was the federal Stored Communications Act (SCA). Enacted in 1986, the SCA governs the disclosure of stored communications and transactional records held by third-party Internet service providers. It limits the ability of the government to compel an ISP to turn over information. It also limits the ability of commercial ISPs to reveal content information to nongovernmental entities.

In 1996, President Bill Clinton signed into law the **Communications Decency Act (CDA)**,[1697] which

way in which they behave once they have found their way into a computer. Not all malware is created by disaffected programmers. Recently, computer security company Symantec announced the discovery of what it called the "world's most sophisticated computer malware."[1696] The software code, named Reign, is a highly sophisticated worm designed to provide backdoor access to computers that it infects. It is virtually undetectable and can modify its own code or simply disappear from infected systems in order to avoid discovery. Cybersecurity experts suspect that it was developed by a Western intelligence agency to target foreign governments and that it may have been in operation for years before its discovery. Reign follows in the footsteps of Stuxnet, a hacking software that was apparently created by Western governments in 2010 to disrupt Iranian computers in that country's nuclear facilities. Similarly, a few years ago, a stealth e-mail virus called *WannaCry* made headlines when it disabled millions of computers around the world. WannaCry fell into the category of "**ransomware**", and its creators demanded payments in Bitcoins to "free" affected machines, and to allow their users to access important data that the ransomware had effectively encrypted. While some experts claimed that the ransomware attacks originated in North Korea, others said that they used software exploits developed by the National Security Agency—which, although highly classified, had been exposed by the hacker group known as Shadow Brokers. Another ransomware program called Adylkuzz, began infecting computers shortly after the *WannaCry* outbreak had been contained. **Figure 15–2** diagrams the anatomy of a ransomware attack.

the use of a computer may be more appropriately prosecuted under "traditional" laws. For that reason, some experts distinguish between computer crime, computer-related crime, and computer abuse. **Computer-related crime** is "any illegal act for which knowledge of computer technology is involved for its investigation, perpetration, or prosecution," whereas **computer abuse** is said to be "any incident without color of right associated with computer technology in which a victim suffered or could have suffered loss and/or a perpetrator by intention made or could have made gain."[1700] The Cybersecurity Enhancement Act of 2014 (whose name is almost identical to the 2002 legislation described earlier) provides for "an ongoing, voluntary public–private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes."

The **Cybersecurity Information Sharing Act of 2015 (CISA)** is designed to improve cybersecurity in the United States by facilitating the sharing of information about cybersecurity threats. It allows for the easy sharing of Internet traffic information between the U.S. government and technology and manufacturing companies.

The purpose of the law is to make it easier for private companies to quickly and directly share personal information with the government, especially in cases involving specific cybersecurity threats.

The law also creates a portal for a variety of federal

In 1996, President Bill Clinton signed into law the **Communications Decency Act (CDA)**,[1697] which sought to protect minors from harmful material on the Internet. A portion of the CDA criminalized the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. Another section prohibited the knowing sending or displaying to a person under 18 any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Shortly after the law was passed, however, the American Civil Liberties Union (ACLU) and a number of other plaintiffs filed suit against the federal government, challenging the constitutionality of the law's two provisions relating to the transmission of obscene materials to minors.

In 1996, a three-judge federal district court entered a preliminary injunction against enforcement of both challenged provisions, ruling that they contravened First Amendment guarantees of free speech. The government then appealed to the U.S. Supreme Court. The Court's 1997 decision *Reno* v. *ACLU*[1698] upheld the lower court's ruling and found that the CDA's "indecent transmission" and "patently offensive display" provisions abridge "the freedom of speech" protected by the First Amendment. Most other federal legislation aimed at keeping online pornography away from the eyes of children has not fared any better when reviewed by the Court. Although the Children's Internet Protection Act (CIPA), which requires public and school libraries receiving certain kinds of federal funding to install pornography filters on their Internet-linked computers, was approved by the justices, most observers acknowledge that the Court has placed the

The History and Nature of Hacking

Audio

Listen to the Audio

Listen to audio

Some authors suggest that computer hacking began with the creation of the interstate phone system and direct distance dialing implemented by AT&T in the late 1950s.[1701] Early switching devices used audible tones that were easily duplicated by electronics hobbyists and "blue boxes" capable of emulating such tones quickly entered the illicit marketplace. **Phone phreaks** used special telecommunications access codes and other restricted technical information to avoid paying long-distance charges. Some were able to place calls from pay phones and others fooled telephone equipment into billing other callers.

Recently, the U.S. Department of Homeland Security (DHS) identified a number of contemporary threats to mobile phones and other handheld devices. According to DHS, "Smartphones' popularity and relatively lax security have made them attractive targets for attackers."[1702] As DHS notes, smartphone security has not kept pace with traditional computer security, and security measures, such as firewalls, antivirus, and encryption, are relatively uncommon on mobile phones. Moreover, mobile phone operating systems are not updated as frequently as those on personal computers, and mobile social networking applications often lack the privacy controls of their PC counterparts. Unfortunately, says DHS, many smartphone users do

avoid paying long-distance charges. Some were able to place calls from pay phones and others fooled telephone equipment into billing other callers.

Recently, the U.S. Department of Homeland Security (DHS) identified a number of contemporary threats to mobile phones and other handheld devices. According to DHS, "Smartphones' popularity and relatively lax security have made them attractive targets for attackers."[1702] As DHS notes, smartphone security has not kept pace with traditional computer security, and security measures, such as firewalls, antivirus, and encryption, are relatively uncommon on mobile phones. Moreover, mobile phone operating systems are not updated as frequently as those on personal computers, and mobile social networking applications often lack the privacy controls of their PC counterparts. Unfortunately, says DHS, many smartphone users do not recognize these security shortcomings, and so they fail to enable the security software that comes with their phones. Users believe that surfing the Internet on their phones is as safe as or safer than surfing on their computers. Increasing the threat, DHS notes, are "recent innovations in mobile commerce that have enabled users to conduct many transactions from their smartphone, such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, banking, processing point-of-sale payments, and even paying at cash registers."[1703]

See **https://ssrn.com/abstract=1363932** for a discussion of self-defense in cyberspace.

A Profile of Cybercriminals

15.5 Describe the characteristics of cybercriminals.

Audio

Listen to the Audio

Listen to audio

Cybercriminals come from a diverse background and cybercrime can run the gamut from simple computer hacking to far more malicious activities. In 2014, for example, Tevon Harris aka "Da Kidd" and "King Kidd," 22, of Houston, was convicted of trafficking children under the age of 18 for commercial sex and sentenced to 40 years in federal prison. Harris was also ordered to spend the rest of his life on supervised release and must register as a sex offender.[1704]

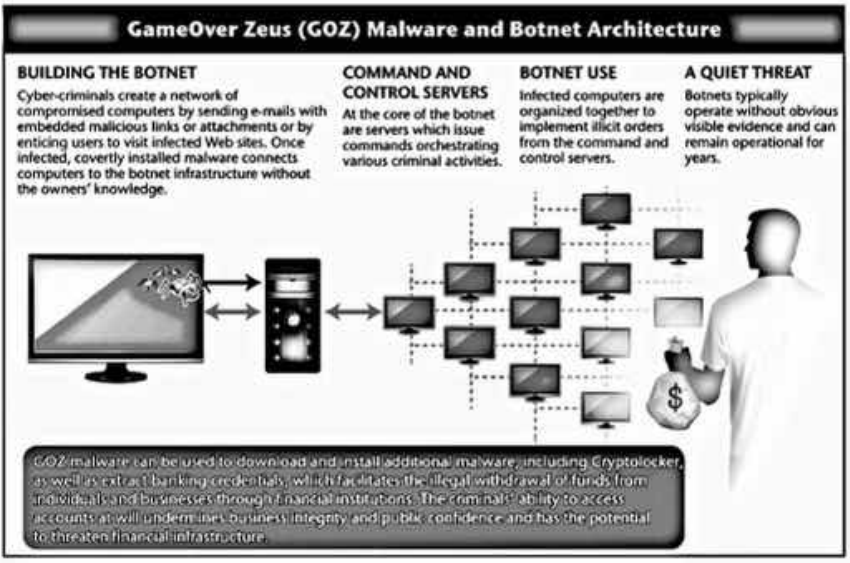
Prior to his 2012 arrest, Harris forced young girls, whom he met on social networking sites, into prostitution. His scheme involved promises of a modeling career. Instead Harris arranged to pick them up, then took them to motel rooms where he forced them to have sex with him. He used violence to keep the girls compliant and deprived them of food, while supplying them with drugs and alcohol. The victims were photographed and their images were posted in online ads for prostitution.

A less violent, but still serious, offense led to the 2014 indictment of Evgeniy Mikhailovich Bogachev of Anapa (part of the Russian Federation). Bogachev was

(part of the Russian Federation). Bogachev was charged by U.S. officials with administering the GameOver Zeus botnet.[1705] A botnet is a global network of infected computers that can be used for illegal purposes (**Figure 15–4**). Bogachev used personal cyberskills that he had acquired during his youth to steal banking credentials from financial institutions and then wired as much as $100 million to overseas accounts.

FIGURE 15-4

Botnet Architecture



Source: Federal Bureau of Investigation.

The indictment of Bogachev illustrates both the potential for high-technology offenders to thwart government efforts at prosecution by operating internationally as well as the transnational nature of hacker subculture. It is from hacker subculture that cybercriminals tend to come because hackers and hacker identities are the products of cyberspace, a realm that exists only within electronic networks where computer technology and human psychology meet. For many hackers, cyberspace provides the opportunity for impersonal interpersonal contact, technological

challenges, and game playing. Fantasy role-playing games are popular among hackers and may engross many "wave riders," who appear to prefer what is called "virtual reality" to the external physical and social worlds around them: "Cyberspace is hacker heaven." *1706*

No one knows the actual identity of many of these people, but computer-security experts have come up with a rough profile of the average hacker.*1707* He is a male between the ages of 16 and 25 who lives in the United States, is a computer user but not a programmer, and hacks with software written by others; his primary motivation is to gain access to Web sites and computer networks, not to profit financially (see the Who's to Blame box in this chapter).

Hackers can be distinguished both by their purpose and by their method of operation, but such categorization is descriptive; distinctions can also be made on the basis of personality and lifestyle. Some experts have suggested that hackers can be grouped according to psychological characteristics:*1708*

- **Pioneers.** Individuals who are fascinated by the evolving technology of telecommunications and explore it without knowing exactly what they are going to find are called pioneers; few hard-core criminals are found among this group.
- **Scamps.** Hackers with a sense of fun, with no intention to harm, are referred to as scamps.
- **Explorers.** Explorers are hackers motivated by their delight in discoveries associated with

- **Explorers.** Explorers are hackers motivated by their delight in discoveries associated with breaking into new computer systems—the farther away geographically such systems are from the hackers' physical locations or the more secure such systems are, the greater the excitement associated with breaking into them.

- **Game players.** Game players enjoy defeating software or system copy protection and may seek to illegally access computer systems with games to play. Hacking itself becomes a game for this sort of hacker.

- **Vandals.** Malicious hackers who deliberately cause damage with no apparent gain for themselves are called vandals. The original 414 Gang in Milwaukee, which broke into the Sloan-Kettering Cancer Institute's computers and wiped out patient records, is an example of this type of hacker.

- **Addicts.** Classic computer nerds who are addicted to hacking and to computer technology are addicts. They may also be addicted to illicit drugs (some hacker bulletin board systems post information on drugs as well as on modems, passwords, and vulnerable systems).

Psychologist Percy Black argued for the existence of an underlying theme in all cases of hacking, calling it "the search for a feeling of power, possibly stemming from a deep-seated sense of powerlessness."[1709] Hacking may serve as compensation for feelings of personal inferiority; by challenging the machine and by winning against machine culture, hackers go through a kind of

against machine culture, hackers go through a kind of rite of passage into adulthood, whereby they prove themselves capable of success.

Because most hackers are young adolescent males, it is important to realize that "their other favorite risky business is the time-honored adolescent sport of trespassing. They insist on going where they don't belong. But then teen-age boys have been proceeding uninvited since the dawn of human puberty. It seems hard-wired. The only innovation is in the new form of the forbidden zone and the means of getting in it."[1710]

Unfortunately, not all computer hackers are simply kids trying their hand at beating technological challenges. Many are "high-tech computer operators using computers to engage in unlawful conduct."[1711] Learn more about hackers and information security at the CERT Coordination Center, which can be reached via **https://www.cert.org/**.

Crime in the News

Cyberbanging

Recently, a new term, *cyberbanging*—referring to the use of the Internet and social networking Web sites by street gangs to tout their exploits, recruit new members, post threats, and socialize—entered the law enforcement lexicon. Videos and lyrics glorifying gang activities can be found on Facebook, MySpace, and Twitter, and some gangs have their own home pages and even run their own servers. "Gangs are going to use any form of communication they can," stated

use any form of communication they can," stated George W. Knox, director of the National Gang Crime Research Center, "including Twitter, including Facebook." Law enforcement experts have said that gangs sometimes use social networking sites to circumvent court injunctions forbidding members from meeting face-to-face.

One study of Internet gang activity, however, found that gangs are not using the Web to recruit new members or to commit cybercrimes. Instead, they "are doing online what they are doing on the street," the study found. That means that they are using sites like Facebook, Twitter, and YouTube for self-promotion, bragging, and making territorial claims. According to study authors, the virtual world is viewed by gang members as another territory, or turf, on which to post electronic graffiti, gang signs, and images. The study was based on interviews with 585 young adult gang members from five cities.

Police agencies and criminal prosecutors have begun scouring social networking sites looking for evidence they can use to disrupt gang activities or to prosecute gang members for crimes they've committed. "Five years ago we would find evidence in a gang case on the Internet and say, 'Wow!'" Bruce Riordan, director of antigang operations for the Los Angeles City Attorney's office commented. "Well, there's no more 'Wow' anymore. It's much more routine."

Discussion Questions

1. What is cyberbanging? What purpose does it serve?

2. Can you imagine any new and innovative ways in which gangs might make use of the

Discussion Questions

1. What is cyberbanging? What purpose does it serve?

2. Can you imagine any new and innovative ways in which gangs might make use of the Internet and social media?

A prisoner charged with murdering a corrections officer who took him to a hospital appointment in Utah. Curtis Allgier, a neo-Nazi affiliated with the Aryan Brotherhood, is alleged to have wrestled the guard's gun from him and shot him; he then carjacked a vehicle and led police on a chase before being apprehended. Why are street gangs turning to the Internet?
Splash News/Newscom

Sources: Tony Castro, "Valley Gangs Leave Trail on Web," *Los Angeles Daily News*, December 5, 2009, **http://www.dailynews.com/news/ci_13931149** (accessed May 12, 2012); "Study Explores Gang Activity on the Internet," *Science Codex*, March 26, 2013, **http://www.sciencecodex.com/study_explores_gang_activity_on_the_internet-109243** (accessed May 22, 2013); and David C. Pyrooz, Scott H. Decker, and Richard K. Moule, "Criminal and

Cybercrime as a Form of White-Collar Crime

Audio

Listen to the Audio

Listen to audio

Numerous analysts have suggested that cybercrime is merely a new form of white-collar crime or maybe its ultimate expression (white-collar crime is discussed in detail in **Chapter 13**). Donn B. Parker, author of the National Institute of Justice (NIJ) *Computer Crime: Criminal Justice Research Manual*, compared white-collar criminals with computer criminals, stating that both share certain "common criminal behavior-related issues":[1712]

- Both types of acts are often committed through nonviolent means, although certain industrial, consumer, and environment-related crimes have life-threatening consequences.
- Access to computers or computer storage media, through employment-related knowledge or technical skills, is often needed.
- These acts generally involve information manipulations that either directly or indirectly create profits or losses.
- These crimes can be committed by an individual, by several individuals working in collusion, or by organizations, with the victims in the last case ranging from individual clients to customers to employees in other

media, through employment-related knowledge or technical skills, is often needed.

- These acts generally involve information manipulations that either directly or indirectly create profits or losses.
- These crimes can be committed by an individual, by several individuals working in collusion, or by organizations, with the victims in the last case ranging from individual clients to customers to employees in other organizations.

See the Criminal Profiles box for the story of a convicted hacker who became an author.

According to Parker, cybercrime and white-collar crime also share the following similarities:

- These crimes are difficult to detect, with discovery often started by accident or by customer complaint rather than as the result of direct investigation.
- The general public views many of these acts as less serious than crimes involving physical violence.
- These crimes cost individuals, organizations, and society large amounts of money and other resources.
- Prevention of these crimes requires a combination of legal, technical, managerial, security, and audit-monitoring controls.

Technology in the Fight against Crime

15.6 What new technologies are being used in today's fight against crime?

Audio

Listen to the Audio

Listen to audio

Technology is a double-edged sword: It arms evildoers with potent new weapons of crime commission, yet it provides police agencies and criminal justice personnel with powerful tools useful in the battle against crime. Criminally useful or evasive technologies and law enforcement capabilities commonly leapfrog one another. Consider traffic radar, which has gone from early alwayson units through trigger-operated radar devices to today's sophisticated laser-based speed-measuring apparatus—each change being an attempt by enforcement agencies to keep a step ahead of increasingly sophisticated radar-detection devices marketed to drivers. Radar-jamming devices and laser jammers are also now used by people apparently intent on breaking speed-limit laws. Not to be outdone, suppliers to law enforcement agencies have created radar- detector detectors, which are used by authorities in states where radar detectors have been outlawed.[1713]

Other potent technologies in law enforcement today are computer databases of known offenders (including public access to sex- offender databases), machine-based expert systems, cellular communications, video

based expert systems, cellular communications, video surveillance (often combined with face-recognition technology), electronic eavesdropping, deoxyribonucleic acid (DNA) analysis, and less-lethal weapons. Transponder-based automated vehicle location (AVL) systems now use patrol car–based transmitters in tandem with orbiting global positioning system (GPS) satellites to pinpoint locations of police vehicles to within 50 feet so that dispatchers can better allocate available resources on a given shift and be able to substantially reduce police response times in crisis situations. (Chip-based transponders are also installed in private vehicles to deter thieves and to help trace stolen automobiles.)

In jurisdictions with computer-aided dispatch (CAD) systems, police dispatchers are prompted by computers for important information that allows them to distinguish a location (such as a particular McDonald's). CAD systems also quickly provide information about how often officers have been called to a given site and can tell responding officers what they might expect to find based on past calls from that location.

More innovative crime-fighting technologies are becoming available. The "Spiderman snare," being tested for its usefulness in incapacitating fleeing suspects, is a 16-foot-wide net that is compressed into a small shotgun-like shell. The net has small weights at its circumference and wraps itself around its target after being fired. The snare's impact is harmless, and test subjects report being able to watch with open eyes as the net wraps around them. Another example is a special-frequency disco-like strobe light which quickly

special-frequency disco-like strobe light which quickly disorients human targets by causing intense dizziness, leaving subjects unable to resist cuffing and arrest (operators wear special glasses designed to counter the influence of the light). Because high-speed chases pose a substantial danger to the public, scientists have developed an electromagnetic pulsing device that can be used to temporarily disable a vehicle's electrical system, causing the engine to stall. The prototype is said to be safe enough to use on vehicles driven by those wearing pacemakers.

As new technologies are developed, their potential usefulness in law enforcement activities is evaluated by the FBI, the NIJ, and other agencies. The NIJ's Technology Assessment Program (TAP) focuses on four areas of advancing technology: protective equipment, such as bulletproof vests and other body armor; forensic sciences, including advances in DNA technology; transportation and weapons, such as electronic stun guns and other less-lethal weapons; and communications and electronics, including computer security and electronic eavesdropping.

Recently, the U.S. Department of Justice's National Law Enforcement and Corrections Technology Center (NLECTC) began testing a high-power compact microwave source designed for vehicle immobilization.[1714] The microwave beam emitted by the device can interfere with an automobile's computer circuitry, effectively shutting down a car's engine from up to 35 feet away. As the technology is improved, the device will likely become operable over longer distances, and it may soon become a routine tool in police work.

DNA Technology

Audio

Listen to the Audio

Listen to audio

In April 2018, Joseph James DeAngelo, 72, was arrested in Citrus Heights, California, and charged with being the Golden State Killer (GSK).[1715] The GSK had committed more than 150 residential burglaries, 50 rapes, and 12 murders in Northern California over decades, starting in the mid-1970s. Although police had gathered DNA evidence from GSK crime scenes over the years, they could not find a "match" in DNA databases. So, they turned to GEDmatch, an online ancestry company, and sent DNA samples known to have come from the GSK in for analysis. Although no exact matches were found, analysis revealed a number of close relatives to the killer who were still living in California. After a bit of investigative work, detectives narrowed their focus to family members of the right age and gender. Soon, DeAngelo was identified as a suspect, and crime scene technicians collected his DNA from personal items that he had discarded. DeAngelo's DNA perfectly matched the DNA that had been left behind at crime scenes by the GSK—and he was quickly arrested. DeAngelo, who had once worked as a police officer, and was described by neighbors as "odd" with a loud voice and mean temper, had been tracked down 40 years after his crime spree began through the creative use of **DNA profiling**.

A person's genetic code is contained in his or her DNA,

A person's genetic code is contained in his or her DNA, providing a DNA profile whose composition is unique to each individual (except in the case of identical twins). DNA samples taken from blood, hair, semen, saliva, or even small flakes of skin left at the scene of a crime can be used in DNA profiling. After processing, DNA profiles appear like bar codes on film negatives, codes that can exonerate a suspect or provide nearly irrefutable evidence of guilt.

DNA evidence is long lasting—fossilized DNA is now being used to reconstruct genetic maps of long-extinct plant and animal species. Although DNA analysis is theoretically possible using only a single cell, most reputable DNA laboratories require a considerably greater quantity of material to conduct an effective analysis, but that could change. Using a Nobel Prize–winning technique called "polymerase chain-reaction technology," minute strands of DNA can be effectively amplified so that even the identity of a person taking a single puff from a cigarette can be accurately established from the trace DNA left on the cigarette. With costs dropping, these technological advances are expected to soon be available to a range of forensic analysts.

The National Research Council has called DNA profiling "a highly reliable forensic tool" but admits that it is not infallible.[1716] Obvious differences in scrutinized DNA samples can easily eliminate a suspect, but testing provides less certainty with positive identification, with human error in conducting the tests being perhaps the greatest threat to reliable results. More than 20 states and the federal government generally accept DNA evidence in criminal trials. Other

generally accept DNA evidence in criminal trials. Other jurisdictions, including California, are less clear in their recognition of DNA testing, and trial judges in those states may offhandedly exclude the use of such evidence when experts disagree as to its validity.

In 1993, the U.S. Supreme Court, in the civil case of *Daubert* v. *Merrell Dow Pharmaceuticals, Inc.*, revised the criteria for the admissibility of scientific evidence;[1717] the ruling rejected the previous admissibility standard established in the 1923 case of *Frye* v. *United States*.[1718] The *Daubert* Court ruled that the older *Frye* standard, requiring "general acceptance" of a test or procedure by the relevant scientific community, "is not a necessary precondition to the admissibility of scientific evidence," which is established by Rule 402 of the *Federal Rules of Evidence*, published after *Frye* and superseding it. Rule 402 says that "all relevant evidence is admissible [in a trial], except as otherwise provided by the Constitution of the United States, by Act of Congress, by these Rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority."[1719] The Court said that although "the *Frye* test was displaced by the Rules of Evidence, [it] does not mean that the Rules themselves place no limits on the admissibility of purportedly scientific evidence. Nor is the trial judge disabled from screening such evidence. To the contrary, under the Rules the trial judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable." The real test for the admissibility of scientific expert testimony is for the trial judge to decide "at the outset whether the expert is proposing to testify to (1) scientific knowledge that (2)

will assist the trier of fact to understand or determine a fact in issue." The Court concluded that the trial judge's task is one of "ensuring that an expert's testimony both rests on a reliable foundation and is relevant to the task at hand. Pertinent evidence based on scientifically valid principles will satisfy those demands."

The plaintiffs in *Daubert* were not arguing the merits of DNA testing but were claiming that the drug Bendectin caused birth defects, but the **Daubert standard** eased the criteria for the introduction of scientific evidence at both civil and criminal trials—and effectively cleared the way for the use of DNA evidence in the courtroom.[1720] The *Daubert* Court found that the following factors may be used to determine whether a form of scientific evidence is reliable:

- It has been subjected to testing.
- It has been subjected to peer review.
- It has known or potential rates of error.
- It has standards controlling application of the techniques involved.

One observer, discussing the quality of DNA identification methods, noted, "The challenges today are no longer technical; instead they lie in taking the technology and building a meaningful legal infrastructure around it."[1721] As DNA evidence is accepted throughout jurisdictions nationwide and worldwide, digitized forensic DNA databases (similar to widely used fingerprint archives) are useful at the state and national levels, and most of the states and the federal government (through the FBI laboratory)

federal government (through the FBI laboratory) already have them. In 1998 the FBI announced that its National DNA Index System (NDIS)—which enables U.S. forensic laboratories to exchange and compare DNA profiles electronically, thereby linking unsolved serial violent crimes to each other and to known offenders—had begun operation.[1722] Shortly thereafter, all 50 states had passed legislation requiring convicted offenders to provide samples for DNA databases, and all states have been invited to participate in NDIS. The federal DNA Identification Act of 1994 authorized the FBI to establish DNA indexes for (1) offenders convicted of crimes, (2) samples recovered from crime scenes, and (3) samples recovered from unidentified human remains.[1723] Today, the National DNA Index System is administered under the FBI's Combined DNA Index System (CODIS) and the combined database is known as the CODIS/NDIS. CODIS/NDIS contained around 13 million offender profiles at the start of 2017. The Web-available CODIS/NDIS interactive map with available statistical tables are found in **Figure 15–5**.

Figure 15-5

A Map-based Interface Allowing Access to the FBI's CODIS/NDIS statistics.

Source: FBI.

In 1995 the British police, operating under a new nationwide crime bill, became the first national police force in the world to begin routine collection of DNA samples from anyone involved in a "recordable" offense (a serious crime).[1724] It appears that genetic profiling will become one of the most significant crime-fighting technologies of the twenty-first century. "Genetic profiling—the use of biotechnology to identify the unique characteristics of an individual's DNA—is about to become as prevalent as the Breathalyzer and more important than the fingerprint."[1725]

In 1996, the NIJ released a comprehensive report, titled *Convicted by Juries, Exonerated by Science*, on the applicability of DNA testing to criminal case processing, calling DNA testing "the most important technological breakthrough of twentieth-century forensic science" and providing a detailed review of 28 cases in which postconviction DNA evidence exonerated defendants who had been sentenced to lengthy prison terms.[1726] The 28 cases were selected on the basis of a detailed examination of records that indicated the convicted defendants might have actually been innocent. The men in the study had served, on average, seven years in prison, and most had been tried and sentenced prior to the widespread availability of reliable DNA testing. More and more defense attorneys in court-appointed cases are filing motions for DNA testing and requesting that states pay for the tests.[1727]

It is important to note that a growing number of jurisdictions are requiring the gathering of DNA information from arrestees, and in 2013 the U.S. Supreme Court held, in the case of *Maryland v. King*

information from arrestees, and in 2013 the U.S. Supreme Court held, in the case of *Maryland* v. *King*, that "When officers make an arrest supported by probable cause ... and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."[1728] Finally, the federal Rapid DNA Act of 2017 permits law enforcement agencies to use new quick scan technology that can analyze DNA samples in as little as 90 minutes. Critics of the law say that the results are not as accurate as those produced by traditional laboratory analysis.

Learn more about the science behind forensic DNA testing and how it has been used to convict as well as exonerate criminal defendants at **https://science.howstuffworks.com/life/genetic/dna-evidence.htm**.