

CRIMINOLOGY B:

CHAPTER 14

TEXT "Criminology the Core" by Larry J. Siegel

Course of Study Designed and Constructed by Dr. M. Scott

SECTION 1: Pages 453 – 462 (3 Pages of Hand Written Notes)

"Chapter Outline" to "Cyber Vandalism: Cybercrime with Malicious Intent"

SECTION 2: Pages 462 – 470 (4 Pages of Hand Written Notes)

"Cyber Vandalism" to "The Extent and Costs of Cybercrime"

SECTION 3: Pages 470 – 481 (5 Pages of Hand Written Notes)

"The Extent and Costs of Cybercrime" to "Thinking Like a Criminologist"

***HEADINGS for ALL written work should follow the example below:**

Criminology A

(Course Title)

Student Name: _____


(First & Last)

Chapter / Section

Class Period: _____

TAKING NOTES: Approaches & Strategies: Teach Yourself How to Learn!

The Classic Approach

Gather the Important Data
Target Reading! 

WHO: Name the Players

WHERE: Geography

WHAT: Vocabulary

HOW: Actions & Process

WHEN: Dates in Order

WHY: Reasons

"In Your Own Words!!!"

The Personalized Approach "Summarize"

TRANSLATE
"Text Book"
English to
YOUR English

Copying "Word For Word" does **NOT** insure Understanding

TRANSLATION and SUMMARISING INSURES UNDERSTANDING

"Knowing ≠ Understanding just as Understanding ≠ Knowing" - Doc

Q & A: WRITTEN SUBMISSIONS

CREATE FIVE (5) Questions and Correct Answers for EACH SECTION

Questions should be related to the material being studied.

The questions should be written as if YOU were explaining the material to another person and wanted to see if they understood the Content of the Course.

Questions 1 – 3 should be “BASIC and FACTUAL”

(Vocabulary and/or Basic Information – “*Who, What, When & Where*”)

Questions 4 & 5 should require demonstration of “DEEPER UNDERSTANDING”

(Explain, Compare & Contrast – “*Why & How*”)

The Questions YOU CREATE should be labeled and numbered clearly.

ANSWERS to each question should be written on a new line – just below the question.

For Example: Let's say the topic we were talking about was “*Chickens*.”

(It won't be – but I don't want to give away answers from a topic we WILL be discussing),

GOOD “Q & A” Assignments would look like this:

Criminology A
Chapter 1: Section C

Dr. Scott
Period 9

Q1. “**What is a chicken?**” (Basic Vocabulary – *What?*)

A1. A bird of the clucking variety that many people find delicious.

Q2. “**Who usually raises chickens?**” (Basic Fact – *Who?*)

A2. Usually farmers but sometimes people who like to keep them as pets.

Q3. “**Where are chickens usually raised?**” (Geography - *Location*)

A3. In coops found on farms that often times have business relationships with fast food chains and grocery stores.

Q4. “**Why did the chicken cross the road?**” (Deeper Understanding – *Why?*)

A4. To get to the other side, away from many people who might be hungry.

Q5. “**Explain how a chicken can escape:**” (Deeper Understanding – *How?*)

A5. Using power tools, quick thinking and inspiring an uprising against the oppression of the farmers.

Chapter Outline

Crime in the Cyber Age

Cybertheft: Cybercrime for Profit

Illegal Copyright Infringement
Computer Fraud
Distributing Illegal or Dangerous Services and Materials

Profiles in Crime

THE LOST BOY CASE

Denial-of-Service Attack
Internet Extortion
Internet Securities Fraud
Phishing and Identity Theft
Etailing Fraud
Mass Marketing Fraud

Cybervandalism: Cybercrime with Malicious Intent

Worms, Viruses, Trojan Horses, Logic Bombs, and Spam
Website Defacement
Cyberstalking
Cyberbullying
Cyberspying

Cyberwarfare: Cybercrime with Political Motives

Cyberterrorism
Funding Terrorist Activities

The Extent and Costs of Cybercrime

Controlling Cybercrime

International Treaties
Cybercrime Enforcement Agencies

Transnational Organized Crime

Characteristics of Transnational Organized Crime

Policies and Issues in Criminology

ORIGINS OF ORGANIZED CRIME

Activities of Transnational Organized Crime
The Rise of Transnational Gangs
Controlling Transnational Crime
Why Is It So Difficult to Eradicate Transnational Gangs?

FACT OR FICTION?

- The next war may be conducted in cyberspace.
- Organized crime in the United States is still a local commodity, controlled by five Mafia families in New York City and a few other allied groups in Chicago, Los Angeles, and Miami.

Americans have become very familiar with a previously unknown website called WikiLeaks, an international organization that publishes classified and secret documents that are submitted by unnamed and anonymous sources. Launched in 2006 and run by Julian Assange, an Australian who emigrated to Sweden, WikiLeaks has supporters around the globe. A few years ago, the site began to post videos and documents that had been illegally appropriated from U.S. diplomatic and military computers by unknown hackers. One video showed a 2007 incident in which Iraqi civilians and journalists were killed by U.S. forces. WikiLeaks also leaked more than 76,000 classified war documents from Afghanistan, including U.S. State Department cables. In the aftermath of the leaks, Army Specialist Bradley Manning, 22, was arrested after an informant told federal authorities that he had overheard him bragging about giving WikiLeaks a video of a helicopter assault in Iraq plus more than 260,000 classified U.S. diplomatic cables taken from government computers. Both the U.S. and foreign governments were embarrassed when the confidential cables hit the Net.¹ Bradley Manning (now Chelsea Elizabeth Manning) was convicted under the espionage act and sentenced to up to 35 years in prison.

Wanted on a series of charges stemming from an alleged sexual assault in Sweden and threatened with extradition to the United States to face charges of espionage, Assange was granted asylum by the government of Ecuador and is currently residing in the Ecuadorian embassy in London (his status can change any day and he may be extradited). Despite Assange's physical ►



CONNECTIONS

Chapter 12 reviewed the concept of enterprise crime and its motivations. Cybercrime can be viewed as a type of enterprise crime employing sophisticated technology to achieve illegal profits. It can also enable criminal gangs to engage in global conspiracies involving co-conspirators from around the world.

L01 Discuss the concept of cybercrime and why it has become important.

cybercrime

The theft and/or destruction of information, resources, or funds via computers, computer networks, or the Internet.

transnational organized crime

Criminal conspiracies that cross national and international borders and involve the planning and execution of illicit ventures by groups or networks of individuals working in more than one country.

restriction, WikiLeaks continues to publish secret documents. It made headlines in April 2015 when it published 30,287 documents and 173,132 emails misappropriated from Sony Pictures Entertainment, which allegedly had been stolen by North Korea's intelligence service in revenge for Sony's producing the comedy film *The Interview*, depicting a future overthrow of the North Korean government and the assassination of its leader, Kim Jong-un. Many of the hacked emails proved embarrassing to the studio, including ones mentioning actors' pay and others joking about President Obama and race.

Just a few years ago, complex, global incidents involving leaking classified documents could not have been contemplated, let alone transacted. Innovation brings change and with it new opportunities to commit crime. The technological revolution has provided new tools to misappropriate funds, damage property, and sell illicit material. It has created **cybercrime**, a new breed of offenses that can be singular or ongoing but typically involves the theft and/or destruction of information, resources, or funds utilizing computers, computer networks, and the Internet. The Internet age has also provided new tools and opportunities for criminals to create transnational criminal organizations whose illegal activities span not only national borders but continents. The Internet allows drug traffickers to communicate instantly with buyers around the world, move their product from one nation to another, and ply their trade across continents.

Crime in the Cyber Age

Criminals have become more technologically sophisticated, routinely using the Internet to carry out their criminal conspiracies. The widespread use of computers and the Internet ushered in the age of information technology (IT) and made it an integral part of daily life in industrialized societies. IT involves computer networking, the Internet, and advanced communications. It is the key to the economic system, becoming ever more important as major industries shift their manufacturing plants to areas of the world where production is much cheaper. IT is responsible for the globalization phenomenon, creating transnational markets, politics, and legal systems—in other words, creating a global economy.

The cyber age has also generated an enormous amount of revenue. Worldwide enterprise IT is now more than \$2.5 trillion per year.² More than 3.9 billion individuals and businesses use email, sending more than 190 billion messages per day. Social media sites like Facebook and Twitter are expanding exponentially. Facebook has more than 1.4 billion users; people tweet more than 500 million times a day.³ Magnifying the importance of the Internet is the fact that many critical infrastructure functions are conducted online, ranging from banking to control of shipping on the Mississippi River.⁴ Because of its scope, depth, and usage, the Internet opened up a broad avenue for illegal activity; cybercrime has become a feature of the new millennium.

In addition to cybercrime, the IT revolution has increased the scope of organized criminal enterprises. Criminal organizations that were originally local in scope and activity can now extend their operations from coast to coast and across international borders, hence the term **transnational organized crime**. Integrating IT into their plans, they are able to carry out criminal schemes on a global basis.

This new array of crimes presents a compelling challenge because (a) it is rapidly evolving, with new schemes being created daily, (b) it is difficult to detect through traditional law enforcement channels, and (c) its control demands that agents of the

justice system develop technical skills that match those of the perpetrators. These crimes are vast in scope and place a heavy burden on society. It may even be possible that the recent crime drop is a result of cybercrime replacing traditional street crime. Instead of robbing a bank at gunpoint, contemporary thieves find it easier to hack into accounts and transfer funds to offshore banks. Instead of shoplifting from a brick and mortar store, the contemporary cyberthief joins an international enterprise group that devises clever schemes to steal from retailers. And instead of limiting their criminal escapades to the local population, these transnational gang members now find a whole world of opportunity.⁵

There are actually three general forms of cybercrime. Some cybercriminals use modern technology to accumulate goods and services. **Cybertheft** schemes range from illegally copying material under copyright protection to using technology to commit traditional theft-based offenses such as larceny and fraud.

Other cybercriminals are motivated less by profit and more by the urge to commit **cybervandalism**, or technological destruction. They aim their malicious attacks at disrupting, defacing, and destroying online resources they find offensive.

A third type of cybercrime is **cyberwar** or **cyberterrorism**, which consists of acts aimed at undermining the social, economic, and political system of an enemy nation by destroying its electronic infrastructure and disrupting its economy. This can range from stealing secrets from foreign nations to destroying an enemy's Web-based infrastructure.

Cybertheft: Cybercrime for Profit

In 2014, a Russian national named Aleksandr Andreevich Panin pleaded guilty to a conspiracy charge associated with his role as the primary developer and distributor of SpyEye software. This software was designed specifically to facilitate online theft from financial institutions and enable users to transfer money out of victims' bank accounts and into accounts controlled by criminals. What makes this case unusual was that rather than using SpyEye himself, Panin sold the "product" online. He actually advertised the features of the program, extolling its criminal value. His 150 customers each paid him up to \$8,500 for SpyEye, which they then used to hack into bank accounts and withdraw funds, create bogus credit cards, and engage in other criminal enterprise schemes.⁶

Cyberthieves now have the luxury of remaining anonymous, living in any part of the world, conducting their business during the day or in the evening, working alone or in a group, while at the same time reaching a much wider number of potential victims than ever before. No longer is the con artist or criminal entrepreneur limited to fleecing victims in a particular geographic locale; the whole world can be their target. The technology revolution opened novel methods for cybertheft, ranging from the unlawful distribution of computer software to Internet securities fraud.

Cyberthieves conspire to use cyberspace to distribute illegal goods and services or to defraud people for quick profits. Some of the most common methods are discussed here.

Illegal Copyright Infringement

Ripping off software has become a billion-dollar computer crime because the comparative ease of making copies of computer software has led to a huge illegal market, depriving authors of very significant revenues. Because cyberspace has no borders, software pirates can ply their trade from anywhere in the world and the effects can be devastating to developers. Companies such as Microsoft, Adobe, and Oracle lose billions in yearly revenue from illegal copies of software pirated in and sold abroad.⁷

Groups of individuals work together to illegally obtain software and then "crack" or "rip" its copyright protections before posting it on the Internet for other members

L02 Distinguish among cybertheft, cybervandalism, and cyberterrorism.

cybertheft

The use of computer networks for criminal profits. Copyright infringement, identity theft, and Internet securities fraud are examples of cybertheft.

cybervandalism

Malicious attacks aimed at disrupting, defacing, and destroying technology.

cyberwar/cyberterrorism

Politically motivated attacks designed to compromise the electronic infrastructure of an enemy nation and disrupt its economy.

CHECKPOINTS

Cybercrime is a relatively new breed of offenses that involves the theft and/or destruction of information, resources, or funds utilizing computers, computer networks, and the Internet.

► Criminals have become more technologically sophisticated, routinely using the Internet to carry out their criminal conspiracies.

► The cyber age has generated an enormous amount of revenue.

► The IT revolution has increased the scope of organized criminal enterprises.

► Criminal organizations that were originally local in scope and activity can now extend their operations from coast to coast and across international borders.

► This new array of crimes presents a compelling challenge to law enforcement.

► Cybercrimes are vast in scope and place a heavy burden on society.

L03 Describe the various types of cybercrimes, such as computer frauds, illegal copyright infringement, and identity theft.



AP Images/Shen Shi

Illegal copyright infringement is now a transnational crime. Here, a Chinese officer from the Shenzhen Market Supervision Administration is interviewed outside the office of Shenzhen QVOD Technology after delivering a written decision of administrative penalty to the company. China is slapping the major online provider of pirated videos in the country with a 260 million yuan (US\$42 million) fine. The Shenzhen Market Supervision Administration said that QVOD Technology had distributed a local movie and TV series online without the publishers' permission. The piracy amounted to 86 million yuan in illegal revenue. QVOD had not only repeatedly pirated the content but refused to stop its distribution after being caught. As a result, Chinese authorities levied a fine that was triple the amount of revenue QVOD made from the piracy. QVOD has been facing growing scrutiny from Chinese authorities. The company was found guilty of distributing pornography online and is facing a related police investigation. QVOD rose to notoriety after the company developed peer-to-peer video sharing software called Kuaibo. The software became a popular way for bootleggers to distribute pirated movies and TV shows without paying expensive video bandwidth costs.

warez

A term computer hackers and software pirates use to describe a game or application that is made available for use on the Internet in violation of its copyright protection.

salami slice fraud

Illegally removing small sums from the balances of a large number of accounts and converting them for personal use.

of the group to use; this is called **warez**. Frequently, these pirated copies reach the Internet days or weeks before the legitimate product is commercially available. Even when warez members do not profit from their efforts, they deprive software companies of legitimate revenue.

The government has actively pursued members of the warez community, and some have been charged and convicted under the Computer Fraud and Abuse Act (CFAA), which criminalizes accessing computer systems without authorization to obtain information,⁸ and the Digital Millennium Copyright Act (DMCA), which makes it a crime to circumvent antipiracy measures built into most commercial software and also outlaws the manufacture, sale, or distribution of code-cracking devices used to illegally copy software.⁹

FILE SHARING Another form of illegal copyright infringement involves file-sharing programs that allow Internet users to download music and other copyrighted material without paying the artists and record producers their rightful royalties. Although some students routinely share files and download music, criminal copyright infringement represents a serious economic threat. The United States Criminal Code provides penalties for a first-time offender of five years incarceration and a fine of \$250,000.¹⁰ Other provisions

provide for the forfeiture and destruction of infringing copies and all equipment used to make the copies.¹¹

On June 27, 2005, copyright protection of music and other types of entertainment distributed via the Internet was upheld by the Supreme Court in the case of *MGM Studios, Inc. v. Grokster, Ltd.* Grokster was a privately owned software company that created peer-to-peer file-sharing protocols. The Court unanimously held that software distributors such as Grokster could be sued for inducing copyright infringement if they market file-sharing software that might induce people to illegally copy protected material even if that software could also be used for legitimate purposes. Justice David Souter wrote:

We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by the clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

As a result, Grokster was forced to pay \$50 million to the music and recording industries, which of course ended its operations.¹²

Computer Fraud

There are many schemes that fall under this category of crime. The **salami slice fraud** involves loading programs that skim small sums from each transaction on the

computers of financial organizations such as banks. The “slices” that are then deposited into the conspirators’ account are so small that they bypass bank scrutiny. Typically an inside job, the salami slice relies on the fact that depositors will not notice if a few pennies are missing from their account each month, or if they do, they won’t bother to report it to bank managers.

Other type of computer crimes include:

- *Theft of information.* The unauthorized obtaining of information from a computer (hacking), including software that is copied for profit.
- *Manipulation of accounts/banking systems.* Similar to a salami slice but on a much larger and usually more complex scale. Sometimes perpetrated as a “one-off kamikaze” fraud.
- *Corporate espionage.* Trade secrets are stolen by a company’s competitors, which can be either domestic or foreign. The goal is to increase the rival companies (or nation’s) competitive edge in the global marketplace.¹³

Internal attacks are now outgrowing external attacks at the world’s largest financial institutions. According to one global security survey, about 60 percent of U.S. companies report being hit by computer network attacks each year.¹⁴

THEFT FROM AUTOMATIC TELLER MACHINES Automatic teller machines (ATMs) attract the attention of cybercriminals looking for easy profits. Rather than robbing an ATM user at gunpoint, the cybercriminal relies on stealth and technological skill to commit the crime. **ATM skimming** involves placing an electronic device on an ATM that scoops information from a bank card’s magnetic strip whenever a customer uses the machine; skimmers can then create their own bank cards and steal from customer accounts.¹⁵ ATM skimming now costs U.S. banks hundreds of millions of dollars annually.

The devices planted on ATMs are usually undetectable because they blend right into the ATM’s physical structure. Some cybercriminals attach a phony keypad on top of the real keypad which records every keystroke as customers punch in their PINs. These skimming devices are installed for short periods of time—usually just a few hours—so they’re often attached to an ATM by nothing more than double-sided tape. They are then removed by the criminals, who download the stolen account information and encode it onto blank cards. The cards are used to make withdrawals from victims’ accounts at other ATMs. Skimmers can also make use of a hidden camera, installed on or near an ATM, to record customers’ entry of their PINs into the ATM’s keypad.

ATM skimming

Using an electronic device or camera on an ATM that copies information from a bank card’s magnetic strip whenever a customer uses the machine or photographs their key strokes.

Distributing Illegal or Dangerous Services and Materials

The Internet has become a prime source for the delivery of illicit or legally prohibited material. Included within this market is distribution of pornography and obscene material, including kiddie porn, and the distribution of dangerous drugs.

DISTRIBUTING OBSCENITY The IT revolution has revitalized the porn industry. The Internet is an ideal venue for selling and distributing obscene material; the computer is an ideal device for storage and viewing. It is difficult to estimate the vast number of websites featuring sexual content, including nude photos, videos, live sex acts, and webcam strip sessions among other forms of “adult entertainment.”¹⁶ While it is difficult to estimate the extent of the industry, it is estimated that the revenue generated from adult sites each year is greater than all movie box office sales and the combined income of ABC, NBC, and CBS.¹⁷

While there are no conclusive data on the extent of Internet porn sites, some experts claim that out of the million most popular websites in the world, about 5 percent, more than 42,000, are sex related; about 15 percent of all searches are for “adult” content.¹⁸ That would mean that adult sites get more than 10 billion hits each year. The single most popular adult site in the world is LiveJasmin.com, a webcam site which gets around 32 million visitors a month, or almost 2.5 percent of all Internet

CONNECTIONS

Chapter 13 dealt with public order crimes, including illegal acts that are now being facilitated by the Internet. Cyberspace is being used to illegally distribute prescription drugs, advertise prostitution, and disseminate pornography.

CONNECTIONS

As you may recall, Chapter 13 covered the law of obscenity and noted that few if any cases involve adults. Considering this, do you believe that all pornographic material involving adults should be legalized, no matter how outrageous the subject?

users.¹⁹ But these data may undercount the actual number of adult sites: a search in Google on the word “porn” returned over 418 million pages. People are often directed to these sites through “porn-napping” and “typosquatted” websites. Porn-nappers buy expired domain names of existing sites and then try to sell adult material to people who stumble on them while surfing. Typosquat websites are those where a pornographer has deliberately registered names with typos so that people surfing the Net are directed to pornography sites if they misspell a word or put in the wrong keystroke.²⁰

How do adult sites operate today? There are a number of different schemes in operation:²¹

- A large firm sells annual subscriptions in exchange for unlimited access to content.
- Password services charge an annual fee to deliver access to hundreds of small sites, which share the subscription revenues.
- Large firms provide free content to smaller affiliate sites. The affiliates post the free content and then try to channel visitors to the large sites, which give the smaller sites a percentage of the fees paid by those who sign up.
- Webmasters forward traffic to another porn site in return for a small per-consumer fee. In many cases, the consumer is sent to the other sites involuntarily, which is known in the industry as *mousetrapping*. Web surfers who try to close out a window after visiting an adult site are sent to another web page automatically. This can repeat dozens of times, causing users to panic and restart their computers in order to escape.
- Adult sites cater to niche audiences looking for specific kinds of adult content.

The current legal status of Internet porn is still underdetermined, but images involving adults are typically unregulated. Child pornography is another matter, and violations are prosecuted whenever possible. Nonetheless, there are at least 100,000 sites worldwide that still offer kiddie porn. Section 18 U.S.C. 2257 of the United States Criminal Code requires that porn distributors maintain records showing that all performers were over the age of 18 at the time of the production. In addition, it is illegal to peddle virtual kiddie porn if the seller advertises the images as real or promises to deliver images of children even if they do not really exist.²² Despite some successful prosecutions, it has been difficult to control Internet child pornography simply because offenders are scattered around the world, making identification and arrest difficult. There needs to be significant law enforcement agency cooperation to gather evidence and locate suspects. The difficulty of prosecution and the need for cooperation is illustrated in the Lost Boy case, discussed in the Profiles in Crime feature.

DISTRIBUTING DANGEROUS DRUGS In addition to sexual material, the Internet has become a prime purveyor of prescription drugs, some of which can be quite dangerous when they are used to excess or fall into the hands of minors. While federal law prohibits buying controlled substances such as narcotic pain relievers (e.g., OxyContin), sedatives (e.g., Valium), stimulants (e.g., Ritalin), and anabolic steroids (e.g., Equipoise) without a valid prescription and in many cases a physical examination, there are numerous websites that provide prescriptions written by “cyber doctors” relying on online questionnaires located on rogue websites housed in foreign countries. Drugs delivered by such websites may be the wrong drugs, adulterated or expired, the wrong dosage strength, or have no dosage directions or warnings.²³

How big is the problem? The 2013 prosecution of a single online pharmacy, Pitcairn Internet pharmacy, revealed that it sold more than 14 million doses of Schedule III and IV controlled substances, earning over \$69 million, in the four-year period it operated.²⁴ One study of 159 sites offering drugs for sale found that only two were certified by the National Association of Boards of Pharmacy as legitimate Internet pharmacy practice sites; the other 157 were rogue sites.²⁵ Another problem: there are no controls preventing children from ordering drugs. With access to a credit card, which many kids have, ordering controlled substances online can be rather easy.²⁶

PROFILES IN CRIME

THE LOST BOY CASE

The Lost Boy online bulletin board was established to provide a forum for men who had a sexual interest in young boys to trade child pornography. Law enforcement authorities in the United States and abroad first became aware of the network when Norwegian and Italian authorities discovered that a North Hollywood, California, man was communicating via an Internet site with an Italian national about child pornography and how to engage in child sex tourism in Romania. Further investigation revealed that Lost Boy had 35 members; more than half were U.S. nationals. Other members of the network were located in countries around the world, including Belgium, Brazil, Canada, France, Germany, New Zealand, and the United Kingdom.

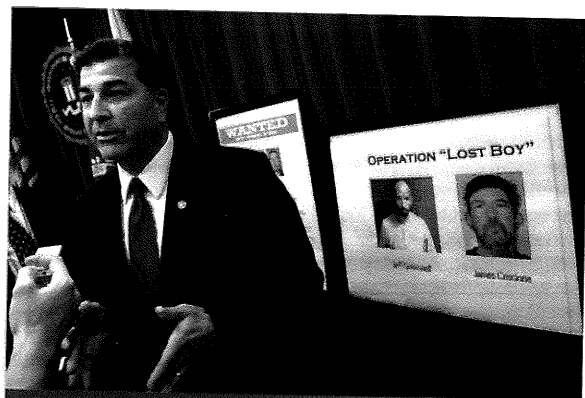
To shield themselves from prosecution, the Lost Boy network had developed a thorough vetting process for new members to weed out law enforcement agents. Members were required to post child pornography in order to join the organization and to continue posting child pornography to remain in good standing. Lost Boy members advised each other on techniques to evade detection by law enforcement, which included using screen names to mask identities and encrypting computer data.

As the investigation unfolded, law enforcement agencies identified child molestation suspects in

South America, Europe, and New Zealand. Suspects in Romania, France, Brazil, Norway, and the United Kingdom were charged and convicted, receiving long prison sentences. In the United States, offenders were prosecuted under the Adam Walsh Child Protection and Safety Act, a 2006 law with a three-tier system of categorizing sex offenders, mandated lifetime sex offender registration for tier one offenders and increased penalties. It also allows judges to levy heavier sentences on child molesters who are engaged in cooperative, sustained criminal efforts with others, such as running the Lost Boy network. Fifteen U.S. Lost Boy defendants have been convicted, one died in custody, and three remain at large. All told, the authorities identified 200 victims as a result of the investigation.

At the time, the Lost Boy indictment was the largest-ever child exploitation enterprise investigation since the signing of the Walsh Act. Because of the sentencing enhancements, some of those prosecuted in the Lost Boy case received sentences of between 20 and 35 years in prison. One man, Jeffrey Greenwell, who produced pornographic images and videos that appeared on the Lost Boy online bulletin board, pleaded guilty to five counts of production of child pornography and was sentenced to a total of 100 years in prison. Since the Lost Boy case was prosecuted, Operation Delego, conducted by the Justice Department and the Department of Homeland Security, resulted in the indictment of 72 defendants for their participation in Dreamboard—a private, members-only, online bulletin board created to promote pedophilia.

The Lost boy case illustrates the difficulty of controlling Internet pornography. Getting evidence sufficient for prosecution involved the cooperation of law enforcement agencies around the world and the arrests of people in multiple countries, a very expensive and time-consuming activity.



Steven Martinez, Assistant Director of the FBI in Los Angeles, speaks to reporters after the Lost Boy international child pornography ring was dismantled.

Gabriel Bouys/Getty Images

Sources: Text of the Adam Walsh Child Protection and Safety Act of 2006, www.govtrack.us/congress/bills/109/hr4472/text; U.S. Department of Justice, "Ohio Man Sentenced to 35 Years in Prison for His Participation in an Online Child Pornography Bulletin Board," www.fbi.gov/losangeles/press-releases/2012/ohio-man-sentenced-to-35-years-in-prison-for-his-participation-in-an-online-child-pornography-bulletin-board (URLs accessed 2015).

**denial-of-service
attack (DoS)**

Extorting money from an Internet service user by threatening to prevent the user from having access to the service.

Denial-of-Service Attack

Used to harass or extort money from owners of an Internet site, a **denial-of-service attack (DoS)** involves threats or attacks designed to prevent the legitimate operation of the site. In some cases, there is no monetary objective and the attack is a type of cybervandalism. In 2015, an attack against Rutgers University interrupted Internet service for students, faculty, and staff; another attack knocked out New York City's email accounts.²⁷ However, some DoS attackers are seeking to extort money from site operators. Unless the site operator pays, the attackers threaten to keep up the interference until real consumers become frustrated and abandon the site. Even so-called respectable businesspeople have been accused of launching denial-of-service attacks against rival business interests.²⁸ Examples of DoS attacks include:

- Attempts to flood a computer network, thereby preventing legitimate network traffic
- Attempts to disrupt connections within a computer network, thereby preventing access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to a specific system or person

Online gambling casinos—a \$20 billion a year international industry—have proven particularly vulnerable to attack. Hundreds of attacks have been launched against online casinos located in Costa Rica, the Caribbean, and Great Britain. If the attack coincides with a big sporting event such as the Super Bowl, the casinos may give in and make payments rather than lose revenue and fray customer relations. Another vulnerable target is online gaming sites. In 2014, massive attacks disrupted service on games such as Blizzard's Battle.net, Riot Games' League of Legends, and the Origin service run by Electronic Arts.²⁹

Internet Extortion

Internet extortion schemes involve uploading malware, attached to an email or compromised website, that freezes a computer and fixes the screen with a pop-up message—supposedly from the FBI or another federal agency—saying that the user has violated some sort of federal law and the computer will remain locked until the victim pays a fine. There may also be a pop-up message saying that personal files have been encrypted and demanding payment to release the decryption codes. The extortionists demand anywhere from hundreds to thousands of dollars to release their hold on the computer. Not only have individuals been the victim of ransomware attacks, so have businesses, financial institutions, government agencies, and academic institutions.

While some of the earlier ransomware scams involved having victims pay the ransom with prepaid credit cards, victims are now increasingly asked to pay with Bitcoin, a decentralized virtual currency network that attracts criminals because of the anonymity the system offers. A fairly new ransomware variant called CryptoWall (and CryptoWall 2.0, its newer version), encrypts files on a computer's hard drive and any external or shared drives to which the computer has access. It directs the user to a personalized victim ransom page that contains the initial ransom amount (anywhere from \$200 to \$5,000), detailed instructions about how to purchase Bitcoins, and typically a countdown clock to notify victims how much time they have before the ransom doubles. Victims are infected with CryptoWall by clicking on links in emails that appear to be from legitimate businesses and through compromised advertisements on popular websites. Recovery can be a difficult process that may require the services of a specialist.³⁰

Internet Securities Fraud

Internet securities fraud involves intentionally manipulating the securities marketplace for profit. There are three major types of Internet securities fraud today:

- *Market manipulation.* Stock market manipulation occurs when an individual tries to control the price of stock by interfering with the natural forces of supply and demand. There are two principal forms of this crime: the **pump and dump** and the **cyber smear**. In a pump and dump scheme, erroneous and deceptive information is posted online to get unsuspecting investors interested in a stock while those spreading the information sell previously purchased stock at an inflated price. The cyber smear is a reverse pump and dump: negative information is spread online about a stock, driving down its price and enabling people to buy it at an artificially low price before rebuttals by the company's officers reinflate the price.³¹
- *Fraudulent offerings of securities.* Some cybercriminals create websites specifically designed to fraudulently sell securities. To make the offerings look more attractive than they are, assets may be inflated, expected returns overstated, and risks understated. In these schemes, investors are promised abnormally high profits on their investments. No investment is actually made. Early investors are paid returns with the investment money received from the later investors. The system usually collapses, and the later investors do not receive dividends and lose their initial investment.
- *Illegal touting.* Individuals make securities recommendations and fail to disclose that they are being paid to disseminate their favorable opinions. Section 17(b) of the Securities Act of 1933 requires that paid touters disclose the nature, source, and amount of their compensation. If those who tout stocks fail to disclose their relationship with the company, information misleads investors into believing that the speaker is objective and credible rather than bought and paid for.

Phishing and Identity Theft

Identity theft occurs when a person uses the Internet to steal someone's identity and/or impersonate the victim to open a new credit card account or conduct some other financial transaction. It is a type of cybercrime that has grown at surprising rates over the past few years.³² In fact, the threat is so real that a recent survey found that the general public would be willing to have their taxes increased in order to fund a program that reduced identity theft.³³

Identity theft can destroy a person's life by manipulating credit records or stealing from bank accounts. Identity thieves use a variety of techniques to steal information. They may fill out change-of-address cards at the post office and obtain people's credit card bills and bank statements. They may then call the credit card issuer and, pretending to be the victim, ask for a change in address on the account. They can then charge numerous items over the Internet and have the merchandise sent to the new address. It may take months for the victim to realize the fraud because the victim is not getting bills from the credit card company.³⁴

Some identity thieves create false emails or websites that look legitimate but are designed to gain illegal access to a victim's personal information; this is known as **phishing** (also known as *carding* and *spoofing*). Some phishers send out emails that look like they come from a credit card company or online store telling the victim there is a problem with their account credit or balance. To fix the problem and update their account they are asked to submit their name, address, phone numbers, personal information, credit card account numbers, and Social Security number (SSN). Once phishers have a victim's personal information, they can gain access to preexisting bank accounts or credit cards and buy things using those accounts or they can use the information to open brand new bank accounts and credit cards without the victim's knowledge. Another variation of this crime is **spear-phishing**, where cybercriminals target specific victims, sending them emails that contain accurate information about their lives, friends, and activities obtained from social networking sites, blogs, or other websites. Personal information makes the message seem legitimate, increasing the chances the victims will open the email or go to a tainted website.³⁵

The cost of phishing and identity theft now runs in the billions. One example of the breadth of the loss can be found in a recent audit of the Internal Revenue Service

pump and dump

Placing deceptive information online to get unsuspecting investors interested in a stock while those spreading the information sell previously purchased stock at an inflated price.

cyber smear

Negative information is spread online about a stock, driving down its price and enabling people to buy it at an artificially low price.

identity theft

Using the Internet to steal someone's identity and/or impersonate the victim in order to conduct illicit transactions such as committing fraud using the victim's name and identity.

phishing

The creation of false emails or websites that look legitimate but are designed to gain illegal access to a victim's personal information.

spear-phishing

Targeting specific victims by using personal information gleaned from social media and then sending them messages that convince them to open tainted emails or go to a tainted website.

(IRS) that found the agency paid refunds to criminals who filed false tax returns, in some cases on behalf of people who had died. In all, the IRS is expected to lose as much as \$21 billion in revenue between 2012 and 2017 due to identity theft.³⁶

To meet the threat of phishing and identity theft, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to make it a federal crime when anyone:

Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.³⁷

Etailing Fraud

etailing fraud

Illegally buying and/or selling merchandise on the Internet.

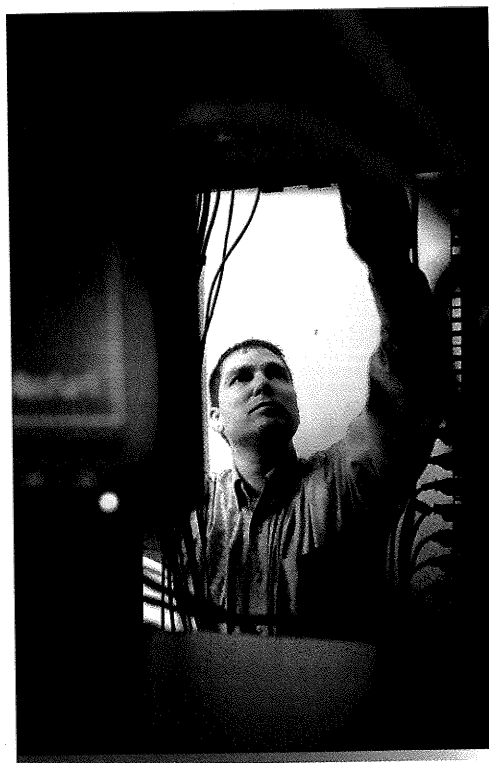
New fraud schemes are evolving to reflect the fact that billions of dollars in goods are sold on the Internet each year. **Etailing fraud** involves illegally buying and/or selling merchandise on the Net. One scam involves purchasing top of the line electronic equipment online and then purchasing a second, similar looking but cheaper model of the same brand. The cheaper item is then returned to the etailer after switching bar codes and boxes with the more expensive unit. Because etail return processing centers don't always check returned goods closely, they may send a refund for the value of the higher priced model.

In another tactic, called *shoplisting*, a person obtains a legitimate receipt from a store either by buying it from a customer or finding it in the trash and then returns to the store and casually shops, picking up identical products. He then takes the products and receipt to the returns departments and attempts to return them for cash, store credit, or a gift card. The thief can sell the gift card on the Internet at a discount for quick cash.

Reshipping frauds are a particularly clever form of etailing crime. Reshippers are recruited in various ways, commonly through employment offers and Internet chat rooms. One scheme involves the posting of help-wanted advertisements at Internet job search sites. The prospective employee is required to complete an employment application that asks for sensitive personal information, such as date of birth and Social Security number, which is then used to obtain credit in his or her name. The applicant is informed he or she has been hired and will be responsible for forwarding, or reshipping, merchandise purchased in the United States to the company's overseas home office. The packages quickly begin to arrive and, as instructed, the employee dutifully forwards the packages to their overseas destination. Unbeknownst to the victim, the recently received merchandise was purchased with fraudulent credit cards obtained using the victim's personal information. Weeks after shipping the merchandise abroad, the victim receives the credit card bill in the mail.³⁸

Mass Marketing Fraud

Mass marketing fraudsters use the Internet to deliver false or deceptive representations to induce potential victims to make advance fee-type payments for services that are never delivered. Exhibit 14.1 sets out some of the more common schemes.



Chris Seward/MCT/Landov

Cyber vandalism can involve extortion schemes, encouraging people to create counter-extortion programs. Craig Petronella has a company in Raleigh, North Carolina, that helps when people or businesses are hit with a computer virus. There is a ransom virus called CryptoLocker going around that locks a computer unless money is paid electronically to the hackers.

Cyber vandalism: Cybercrime with Malicious Intent

2

In 2015, the online hookup site Ashley Madison was hacked, and stolen information from 32 million of the site's members, such as email addresses, was posted on the Net. The hackers claimed two motivations: they objected to Ashley Madison's intent of arranging affairs between

Exhibit 14.1 Common Mass Marketing Schemes

Advance Fee Fraud

This category of fraud induces victims into remitting upfront payments in exchange for the promise of goods, services, and/or prizes. For example:

- In Nigerian letter schemes (also known as “419 scams” because that’s the number of the article in the Nigerian criminal code that deals with these types of frauds), victims are contacted by letter or email with a variety of scenarios that purport to involve the movement of substantial sums of money held in foreign bank accounts. The victims are requested to pay fees to secure the transfer of funds to the United States and in return are promised a large percentage of the transferred funds. Of course, there are no funds and the victims will even be asked to pay additional funds to cover “unanticipated” costs.
- In a foreign lottery/sweepstakes fraud, victims receive emails informing them they have won a substantial prize in a foreign drawing but must remit payment for various taxes/fees to receive their winnings. Alternatively, victims are provided with a counterfeit instrument (such as a cashier’s check) that purports to represent a portion of the winnings. Similar to an overpayment fraud (see below), the victim is told to deposit the check, forward the required payments for taxes/fees,

and the victim can keep the balance. The check is ultimately returned as a counterfeit item and the victim is indebted to their financial institution for the withdrawn funds.

Overpayment Fraud

Victims who have advertised some item for sale via the Internet are contacted by “buyers” who remit counterfeit instruments in excess of the purchase price as payment. The victims are told to cash the instruments, deduct any expenses, and return or forward the excess funds to the “buyer,” but later discover the check was counterfeit. Victims in this fraud not only lose the value of the property sold, but they are also indebted to their financial institutions for the funds withdrawn on the counterfeit check.

Recovery/Impersonation Schemes

Victims are contacted by perpetrators posing as law enforcement officers, government employees, or lawyers who reference the victim’s losses in a prior fraud scheme. Victims are led to believe that the perpetrators have been arrested and funds have been seized to pay back their losses, but of course they must first pay fees for processing and administrative services before the seized funds can be released.

Source: FBI, “Mass Marketing Schemes,” www.fbi.gov/about-us/investigate/white_collar/mass-marketing-fraud (accessed 2015).

married individuals, and they objected to its requirement that users pay \$19 for the privilege of deleting all their data from the site.³⁹ The company issued a \$500,000 reward for the identity of the hackers.

Not all cybercriminals are motivated by greed or profit. Some are motivated by the desire for revenge and destruction or—like the Ashley Madison hackers—some other malicious intent. These are the modern cybervandals. Cybervandalism ranges from sending destructive viruses and worms to stalking or bullying people using cyberspace as a medium:

- Some cybervandals target computers and networks seeking revenge for some perceived wrong.
- Some desire to exhibit their technical prowess and superiority.
- Some wish to highlight the vulnerability of computer security systems.
- Some desire to spy on other people’s private financial and personal information (computer voyeurism).
- Some want to destroy computer security because they believe in a philosophy of open access to all systems and programs.

What forms does cybervandalism take?

Worms, Viruses, Trojan Horses, Logic Bombs, and Spam

The most typical use of cyberspace for destructive intent comes in the sending or implanting of disruptive programs, called viruses, worms, Trojan horses, logic bombs, or spam.

computer virus

A program that disrupts or destroys existing programs and networks, causing them to perform the task for which the virus was designed.

malware

A malicious software program.

computer worms

Programs that attack computer networks (or the Internet) by self-replicating and sending themselves to other users, generally via email without the aid of the operator.

Trojan horse

A computer program that looks like a benign application but contains illicit codes that can damage the system operations. Though Trojan horses do not replicate themselves like viruses, they can be just as destructive.

logic bomb

A program that is secretly attached to a computer system, monitors the network's work output, and waits for a particular signal such as a date to appear. Also called a *slag code*, it is a type of delayed action virus that is set off when a program user makes certain input that sets it in motion. A logic bomb can cause a variety of problems ranging from displaying or printing a spurious message to deleting or corrupting data.

spam

An unsolicited advertisement or promotional material, typically in the form of an unwanted email message. While email is the most common form of spam, it can also be sent via instant messaging, online forum, and mobile phone messaging, among other media.

website defacement

A type of cybervandalism that occurs when a computer hacker intrudes on another person's website by inserting or substituting codes that expose visitors to the site to misleading or provocative information. Defacement can range from installing humorous graffiti to sabotaging or corrupting the site.

VIRUSES AND WORMS A **computer virus** is one type of malicious software program (also called **malware**) that disrupts or destroys existing programs and networks, causing them to perform the task for which the virus was designed.⁴⁰ The virus is then spread from one computer to another when a user sends out an infected file through email, a network, or portable media. **Computer worms** are similar to viruses but use computer networks or the Internet to self-replicate and send themselves to other users, generally via email, without the aid of the operator.

The damage caused by viruses and worms can be considerable. More than a decade ago, the Melissa virus disrupted email service around the world when it was posted to an Internet newsgroup, causing more than \$80 million in damage. Its creator, David Smith, pleaded guilty to state and federal charges and was later sentenced to 20 months in prison (leniency was granted because he cooperated with authorities in thwarting other hackers).⁴¹ Another damaging piece of malware was the MS Blaster worm—also known as W32.Blaster and W32/Lovsan—which took advantage of a vulnerability in a widely used feature of Microsoft Windows and infected more than 120,000 computers worldwide.⁴²

TROJAN HORSES Some hackers introduce a **Trojan horse** program into a computer system. The Trojan horse looks like a benign application but contains illicit codes that can damage the system operations. Sometimes hackers with a sense of irony will install a Trojan horse and claim that it is an antivirus program. When it is opened it spreads viruses in the computer system. Though Trojan horses do not replicate themselves like viruses, they can be just as destructive.

LOGIC BOMBS A fourth type of destructive attack that can be launched on a computer system is the **logic bomb**, a program that is secretly attached to a computer system, monitors the network's work output, and waits for a particular signal such as a date to appear. Also called a *slag code*, it is a type of delayed-action virus that is set off when a program user makes certain input that sets it in motion. A logic bomb can cause a variety of problems ranging from displaying or printing a spurious message to deleting or corrupting data.

SPAM An unsolicited advertisement or promotional material, **spam** typically comes in the form of an unwanted email message; spammers use electronic communications to send unsolicited messages in bulk. While email is the most common form of spam, it can also be sent via instant messaging, online forum, and mobile phone messaging, among other media.

Spam can simply be in the form of an unwanted and unwelcome advertisement. For example, it may advertise sexually explicit websites and get into the hands of minors. A more dangerous and malicious form of spam contains a Trojan horse disguised as an email attachment advertising some commodity such as free software or an electronic game. If the recipient downloads or opens the attachment, a virus may be launched that corrupts the victim's computer; the Trojan horse may also be designed to capture important data from the victim's hard drive and send it back to the hacker's email address. Sending spam can become a crime and even lead to a prison sentence when it causes serious harm to a computer or network.

Website Defacement

Cybervandals may aim their attention at the websites of their victims. **Website defacement** is a type of cybervandalism that occurs when a computer hacker intrudes on another person's website by inserting or substituting codes that expose visitors to the site to misleading or provocative information. Defacement can range from installing humorous graffiti to sabotaging or corrupting the site. In some instances, defacement efforts are not easily apparent or noticeable—for example, when they are designed to give misinformation by substituting or replacing authorized text on a company's web page. The false information may mislead customers and frustrate

their efforts to utilize the site or make it difficult for people using search engines to find the site as they surf the Web.

Almost all defacement attacks are designed to vandalize web pages rather than bring profit or gain to the intruders (though some defacers may eventually extort money from their targets). Some defacers are simply trying to impress the hacking community with their skills. Others may target a corporation when they oppose its business practices and policies (such as oil companies, tobacco companies, or defense contractors). Some defacement has political goals such as disrupting the website of a rival political party or fund-raising group.

Defacers are typically members of an extensive social network who are eager to demonstrate their reasons for hacking and often leave calling cards, greetings, and taunts on web pages.⁴³ It is a worldwide phenomenon. A few years ago, hackers from an organized group called Anonymous defaced hundreds of websites belonging to the Australian government, saying the action was in response to reports of spying by Australia. The websites were defaced with a message reading "Stop Spying on Indonesia." The Anonymous group has also targeted Singapore, Mexico, the Philippines, Australia, Egypt, the United States, Syria, and many more countries.⁴⁴

Website defacement is a significant and major threat to online businesses and government agencies. It can harm the credibility and reputation of the organization and demonstrate that its security measures are inadequate. As a result, clients lose trust and may be reluctant to share information such as credit card numbers and personal information. An e-tailer may lose business if potential clients believe the site is not secure. Financial institutions, such as Web-based banks and brokerage houses, are particularly vulnerable because they rely on security and credibility to protect their clients' accounts.⁴⁵

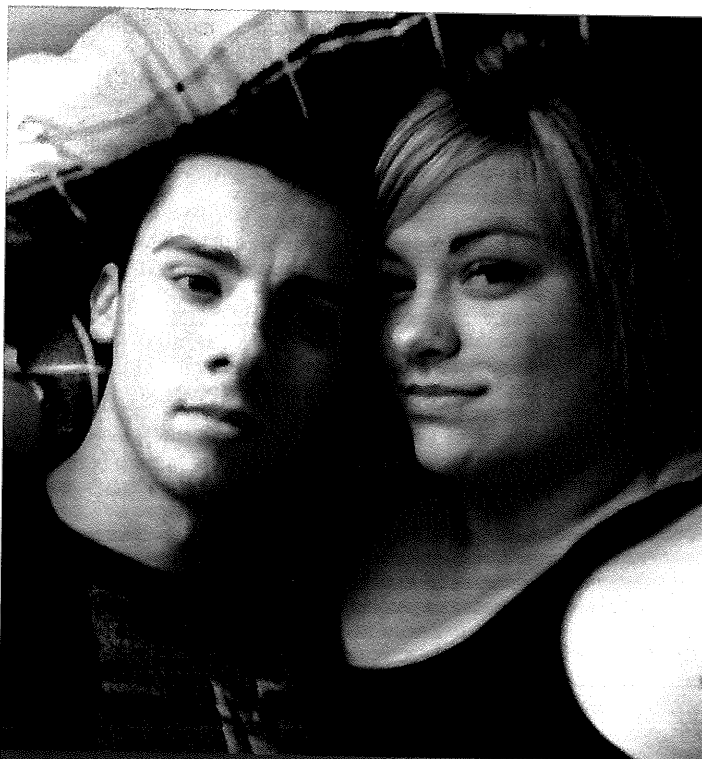
Cyberstalking

Cyberstalking refers to the use of the Internet, email, or other electronic communication devices to stalk another person. Traditional stalking may include following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. In the Internet age, stalkers can pursue victims through online chat rooms. Pedophiles can use the Internet to establish a relationship with the child and later make contact for the purpose of engaging in criminal sexual activities. Today, Internet predators are more likely to develop relationships with at-risk adolescents and beguile underage teenagers than use coercion and violence.⁴⁶

Not all cyberstalkers are sexual predators. Some send repeated threatening or harassing messages via email or text and use programs to send messages at regular or random intervals. A cyberstalker may trick other people into harassing or threatening a victim by impersonating their victim on social media sites, posting messages that are provocative, such as "I want to have sex." The stalker then posts the victim's name, phone number, or email address hoping that other site participants will stalk or hassle the victim without the stalker's personal involvement.

cyberstalking

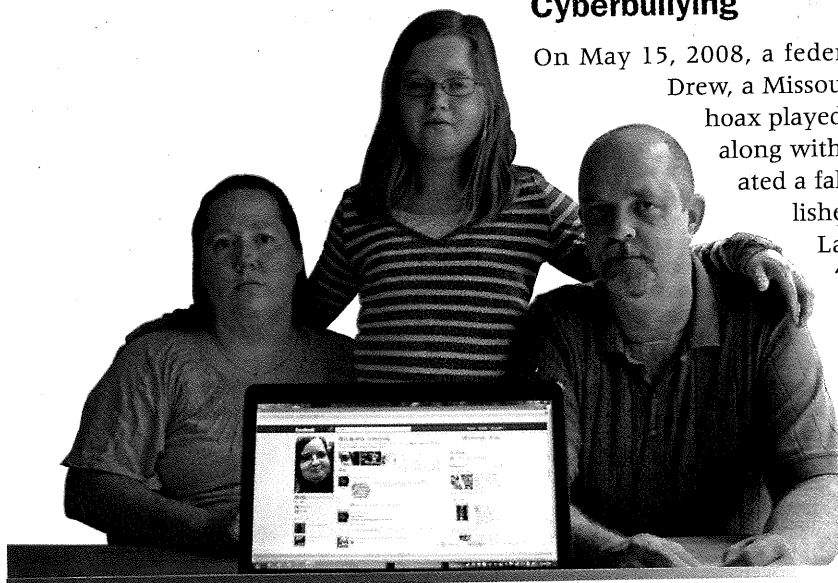
Use of the Internet, email, or other electronic communications devices to stalk another person. Some cyberstalkers pursue minors through online chat rooms; others harass their victims electronically.



HotSpot/Landov

Pictured here are Rebecca Caine, 24, and ex-boyfriend Peter Atkinson, 21, who went on to stalk her for five months after their breakup. Atkinson terrorized Caine, bombarding her with hundreds of texts and calls a day and posting nude pictures of her online. He served just four months in prison for his crimes. Terrified when he was released, Caine was forced to change her job well as her name. She said: "Peter's sentence wasn't long enough. I couldn't be more disappointed. The time he spent in jail is less than the time he spent harassing me. I'm furious."

Cyberbullying



AP Images/David Goldman

Cyberbullying has become common in the United States and has taken its toll on adolescent victims. Here, Alex Boston, 14, poses with her parents, Amy and Chris. In front of them is a screen shot of the phony Facebook account that was set up in Alex's name by two classmates. Alex was humiliated when they stacked the page with phony comments claiming she was sexually active, racist, and involved in drugs.

cyberbullying

Willful and repeated harm inflicted through the medium of electronic text.

cyberspying

Illegally using the Internet to gather information that is considered private and confidential.

On May 15, 2008, a federal grand jury in Los Angeles indicted Lori Drew, a Missouri woman, for her alleged role in a MySpace hoax played on Megan Meier, a teenage neighbor. Drew, along with her daughter and another teenage girl, created a fake online boy named Josh Evans, who established a cyber romance with 13-year-old Megan. Later, after being spurned and attacked by "Josh" on MySpace, Megan took her own life. She had received several messages from "Josh" suggesting that she kill herself and that the "world would be better off without her." Drew was found guilty on three lesser charges (reduced from felonies to misdemeanors by the jury); her conviction was later overturned on appeal.⁴⁷

Megan Meier is one of a number of teens who have taken their lives after being victimized by cyberbullies. While school yard bullying is a well-known problem that remains to be solved, it has now morphed from the physical to the virtual. **Cyberbullying** is defined as the willful and repeated harm inflicted through the medium of electronic text. Like their real-

world counterparts, cyberbullies are malicious aggressors who seek implicit or explicit pleasure or profit through the mistreatment of other individuals.

Because of the creation of cyberspace, physical distance is no longer a barrier to the frequency and depth of harm doled out by a bully to his or her victim.⁴⁸ Although power in traditional bullying might be physical (stature) or social (competency or popularity), online power may simply stem from Net proficiency. Cyberbullies are able to navigate the Net and utilize technology in a way that puts them in a position of power relative to their victim. There are two major formats that bullies can employ to harass their victims: (1) a cyberbully can use a computer and send harassing emails or instant messages, post obscene, insulting, and slanderous messages to social media sites, or develop websites to promote and disseminate defamatory content; (2) a cyberbully can use a cell phone to send harassing text messages to the victim.⁴⁹

How common is cyberbullying? Drs. Sameer Hinduja and Justin Patchin, leading experts on cyberbullying, have conducted yearly surveys using large samples of high school youth. Their most recent effort finds that about 24 percent of the more than 14,000 high school and middle school students they surveyed report having been the target of some form of Internet harassment; similarly, about 17 percent of the students said they have harassed someone via the Internet. Adolescent girls are significantly more likely to have experienced cyberbullying in their lifetimes. The type of cyberbullying tends to differ by gender; girls are more likely to spread rumors while boys are more likely to post hurtful pictures or videos.⁵⁰

Cyberspying

Cyberspying is illegally using the Internet to gather information that is considered private and confidential. Cyberspies have a variety of motivations. Some are people involved in marital disputes who may want to seize the emails of their estranged spouse. Business rivals might hire disgruntled former employees, consultants, or outside contractors to steal information from their competitors. These commercial cyberspies target upcoming bids, customer lists, product designs, software source code, voice mail messages, and confidential email messages.⁵¹ Some of the commercial

spying is conducted by foreign competitors who seek to appropriate trade secrets in order to gain a business advantage.⁵²

Cyberwarfare: Cybercrime with Political Motives

Will future warfare be conducted in cyberspace as well as on the ground? Destroying an enemy's computer network, incapacitating their defense systems, may soon become the opening salvo of hostilities. Sounds fanciful, but there have already been efforts to compromise an enemy's defense industry and military establishment. The most celebrated incident occurred in 2010 when it was widely reported that Iran's efforts to process nuclear material were compromised by a computer worm that infected Iranian nuclear computers and sabotaged the uranium enrichment facility at Natanz—where centrifuge operational capacity suddenly dropped by 30 percent. An attack by the Stuxnet worm was confirmed by the director of the Bushehr facility, whose computers were infected by the virus.⁵³

Iran's military capability is not the only one subject to cyberattack. In 2011, Lockheed Martin, the world's largest aerospace company, announced that it detected and thwarted "a significant and tenacious attack" on its information systems.⁵⁴ Not to worry this time, a company spokesman claimed, because swift action protected the company's secrets. While this attempt at **cyberespionage** did not damage America's military capability, there have been other incidents in which agents have been able to steal top-secret government information.

The Chinese espionage ring known as Titan Rain was able to penetrate the Redstone Arsenal military base and NASA; the U.S. Army's flight-planning software was electronically stolen. Titan Rain agents entered hidden sections of hard drives, zipped up as many files as possible, and transmitted the data to way stations in South Korea, Hong Kong, and Taiwan before sending them to mainland China.⁵⁵ The Pentagon issued a report on China's cyberwarfare capabilities, acknowledging that hackers in China had penetrated the Pentagon's computer system.⁵⁶

Responding to these threats, in 2009 the Secretary of Defense directed the Commander of U.S. Strategic Command to establish the United States Cyber Command (USCYBERCOM), whose duties are stated as:

USCYBERCOM will fuse the Department's full spectrum of cyberspace operations and will plan, coordinate, integrate, synchronize, and conduct activities to: lead day-to-day defense and protection of DoD information networks; coordinate DoD operations providing support to military missions; direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations. The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment.⁵⁷

U.S. Cyber Command went operational on May 21, 2010. In 2011, the U.S. government announced that computer sabotage by another country could constitute an act of war. However, not every attack would lead to retaliation, only those so serious that it would threaten American lives, commerce, infrastructure, or worse, and there would have to be indisputable evidence leading to the nation-state involved.⁵⁸

cyberespionage

Efforts by intelligence agencies to penetrate computer networks of an enemy nation in order to steal important data.



AP Images/Vahid Salemi

Cyberwarfare can be aimed at an enemy nation's infrastructure. Here, an Iranian security guard stands at the Maroun Petrochemical plant at the Imam Khomeini port, in southwestern Iran. Technicians battling a complex computer virus took the ultimate firewall measures, shutting off all Internet links to Iran's oil ministry and the terminal that carries nearly all the country's crude exports.

FACT OR FICTION?

The next war may be conducted in cyberspace.

FACT There have already been a number of cyberattacks on military installations in the United States and abroad.

Cyberterrorism

Cyberspace may also serve as a venue for terrorism. While the term may be difficult to define, cyberterrorism can be seen as an effort by covert forces to disrupt the intersection where the virtual electronic reality of computers meets the physical world.⁵⁹ FBI expert Mark Pollitt defines cyberterrorism as “the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents.”⁶⁰

Terrorist organizations now understand the power that disruption of cyberspace can inflict on their enemies even though, ironically, they may come from a region where computer databases and the Internet are not widely used. Terrorist organizations are adapting IT into their arsenal of terror, and agencies of the justice system have to be ready for a sustained attack on the nation’s electronic infrastructure.

WHY TERRORISM IN CYBERSPACE? Cyberspace is a handy battlefield for the terrorist because an attack can strike directly at a target that bombs won’t affect: the economy. Because technological change plays a significant role in the development of critical infrastructures, they are particularly vulnerable to attack. And because of rapid technological change, and the interdependence of systems, it is difficult to defend against efforts to disrupt services.⁶¹

Cyberterrorists have many advantages. There are no borders of legal control, making it difficult for prosecutors to apply laws to some crimes. Criminals can operate from countries where laws pertaining to cybercrime barely exist, making them almost untouchable. Cyberterrorists can also use the Internet and hacking tools to gather information on targets.⁶² There is no loss of life and no need to infiltrate “enemy” territory. Terrorists can commit crimes from anyplace in the world and the costs are minimal. Nor do terror organizations lack for skilled labor to mount cyberattacks. There are highly skilled computer experts available at reasonable costs in most developing countries.

CYBERATTACKS Has the United States already been the target of cyberterrorism? While it may be difficult to separate the damage caused by hackers from deliberate attacks by terrorists, the Center for Strategic and International Studies has uncovered attacks on the National Security Agency, the Pentagon, and a nuclear weapons laboratory; operations were disrupted at all of these sites.⁶³ There have been numerous attacks and serious breaches in recent years. In addition to the Sony breach mentioned in the opening vignette, such companies as Anthem Health Care, Primera Blue Cross, Staples, and Home Depot have had their computer systems hacked and the names, Social Security numbers, birthdays, addresses, email, and employment information, and income data of current and former customers and employees stolen.⁶⁴ The financial service sector is a prime target and has been victimized by information warfare. In 2013, a massive cyberattack was directed at some of the nation’s largest banks, including JPMorgan Chase, Bank of America, and Citigroup, by a hacker group calling itself Izz ad-Din al-Qassam Cyber Fighters. What made this attack different was that the traffic was coming from data centers around the world that had been infected with a sophisticated form of malware designed to evade detection by antivirus solutions. The bank attackers used those infected servers to simultaneously fire traffic at each banking site until it slowed or collapsed. The purpose of the attack: to punish the American financial system in retaliation for a film insulting to Moslems.⁶⁵

Here are some possible scenarios:

- Logic bombs are implanted in an enemy’s computer. They can go undetected for years until they are instructed through the Internet to overwhelm a computer system.
- Programs are used to allow terrorists to enter “secure” systems and disrupt or destroy the network.
- Using conventional weapons, terrorists overload a network’s electrical system, thereby threatening computer security.⁶⁶

- The computer system of a corporation whose welfare is vital to national security—such as Boeing or Raytheon—is breached and disrupted.
- Internet-based systems used to manage basic infrastructure needs—such as an oil pipeline's flow or water levels in dams—are attacked and disrupted, posing a danger of loss of life and interruption of services.

Terrorists use the Internet to recruit new members and disseminate information. For example, Islamic militant organizations use the Internet to broadcast anti-Western slogans and information. An organization's charter and political philosophy can be displayed on its website, which can also be used to solicit funds. ISIL has recruited young women from Western nations by posting videos on social media sites in which jihadists are introduced as potential husbands. The videos show burka-clad jihadi brides carrying Kalashnikovs and promote the virtues of fighting for the caliphate, telling the women they will receive a "guaranteed ticket to paradise."⁶⁷

Funding Terrorist Activities

Obtaining operational funds is a key to terrorist activity. Terrorist groups use the Internet to raise funds to buy arms and carry out operations.⁶⁸ One method of funding is through fraudulent charitable organizations claiming to support a particular cause such as disaster relief or food services. Using bogus charities to raise money is particularly attractive to cyberterrorists because they face far less scrutiny from the government than for-profit corporations and individuals. They may also qualify for financial assistance from government-sponsored grant programs. One such bogus group, Holy Land Foundation for Relief and Development (HLFRD), provided more than \$12 million to the terrorist group Hamas; in total, HLFRD raised more than \$57 million but only reported \$36.2 million to the IRS.⁶⁹

Bogus companies have also been used by terrorist groups to receive and distribute money. These shell companies may engage in legitimate activities to establish a positive reputation in the business community but produce bills for nonexistent products that are "paid" by another party with profits from illegal activities, such as insurance fraud or identity theft.⁷⁰ If a shell company generates revenues, funds can be distributed by altering financial statements to hide profits and then depositing the profits in accounts that are used directly or indirectly to support terrorist activities.

Another source of terrorist funding, which is discussed less often in the literature, is intellectual property (IP) crime. The illegal sale of counterfeited goods and illegal use of IP to commit other crimes, such as stock manipulation, have been used to support terrorist activities.⁷¹

The various branches of cybercrime are set out in Concept Summary 14.1.

Concept Summary 14.1 Types of Cybercrime

Crime	Definition	Examples
Cybertheft	Use of cyberspace to distribute illegal goods and services or to defraud people for quick profits	Illegal copyright infringement, identity theft, Internet securities fraud, warez
Cyber vandalism	Use of cyberspace for revenge, destruction, and to achieve a malicious intent	Website defacement, worms, viruses, cyberstalking, cyberbullying
Cyberwarfare	An effort by enemy forces to disrupt the intersection where the virtual electronic reality of computers meets the physical world	Logic bombs used to disrupt or destroy "secure" systems or networks, Internet used to communicate covertly with agents around the world. Recruiting for terror groups.

3

3

The Extent and Costs of Cybercrime

How common are cybercrimes, and how costly are cybercrimes to American businesses and the general public? The Internet has become a vast engine for illegal profits and criminal entrepreneurs. An accurate accounting of cybercrime will probably never be made because so many offenses go unreported, but there is little doubt that its incidence is growing rapidly.

Though global business enterprises are subjected to millions of cybercrimes each year, most are not reported to local, state, or federal authorities. Some cybercrime goes unreported because it involves low-visibility acts—such as copying computer software in violation of copyright laws—that simply never get detected.⁷² Some businesses choose not to report cybercrime because they fear revealing the weaknesses in their network security systems.

Despite this reluctance to report cyberattacks, there are growing indications that the cost of cybercrime already outstrips the losses attributed to common-law crimes such as burglary and robbery and is growing at a faster pace. It is now estimated that the cost of cybercrime will reach at least \$2 trillion per year by 2019.⁷³

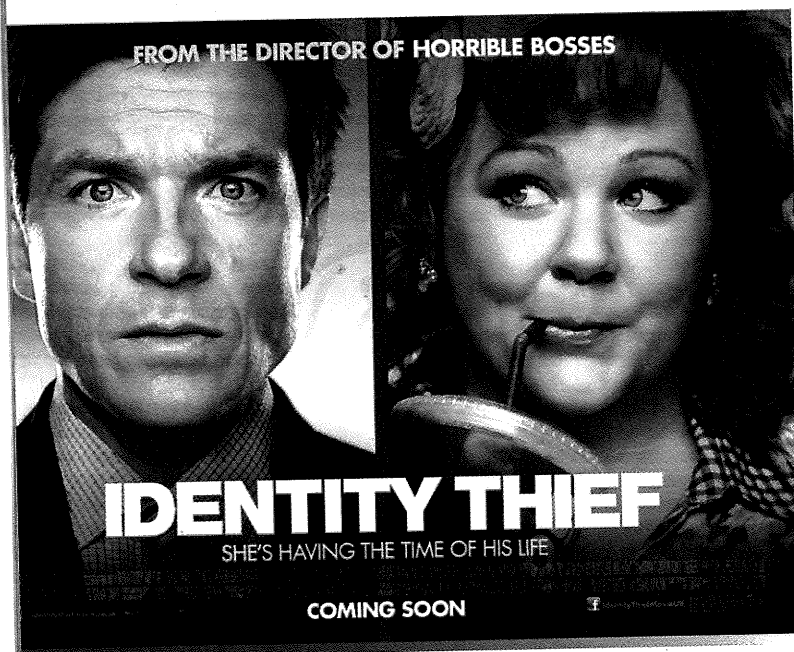
A significant portion of cybercrime costs are borne by business enterprise. File sharing and the illegal reproduction and distribution of movies, software, games, and music now cost U.S. businesses an estimated \$58 billion in annual economic output and more than 300,000 jobs each year.⁷⁴ One reason is the increased computer and Internet usage in emerging economies such as China, Eastern Europe, and Brazil, where piracy rates are highest.⁷⁵

Not only are business enterprises the target of cybertheft, but they also lose billions each year to cybervandalism.⁷⁶ Symantec Corporation (publisher of Norton Antivirus) conducts an annual Internet security threat report that makes use of data from more than 24,000 security devices deployed in more than 180 countries.⁷⁷ According to Symantec, attackers trick companies into infecting themselves with Trojan horse software updates to common programs and patiently wait for their targets to download the malware. Once a victim has downloaded the software update, attackers are given unfettered access to the corporate network. Highly targeted spear-phishing attacks are a favorite tactic for infiltrating networks, as the total number of attacks rose

8 percent between 2013 and 2014. Attackers use stolen email accounts from one corporate victim to attack other victims higher up the food chain. They are learning to take advantage of companies' management tools and procedures to move stolen intellectual property around the corporate network before exfiltration.

The Symantec survey confirmed the prevalence and continued growth of malware, which increased 26 percent in 2014. In fact, there were more than 317 million new pieces of malware created in that year alone—that's nearly one million per day. A sizable portion of all software is now being installed without proper licensing, especially in emerging economies, where unlicensed software use is widespread.

Business enterprise is not the only target that bears the cost of cybercrime. Individuals are also targets, and the costs are high. Take for instance identity theft or phishing. The Internal Revenue Service (IRS) found that the agency paid refunds to criminals who filed false tax returns, in some cases on behalf of people who had died. In all, the IRS is expected to lose as much as \$21 billion in revenue between 2012 and 2017 due to identity theft.⁷⁸



Identity theft has become so pervasive that it is now the fodder of films and books, including the hit 2013 movie *Identity Thief* with Jason Bateman and Melissa McCarthy.

Controlling Cybercrime

The proliferation of cybercrime and its cost to the economy have created the need for laws and enforcement processes specifically aimed at controlling its emerging formulations. Because technology evolves so rapidly, the enforcement challenges are particularly vexing. There are numerous organizations set up to provide training and support for law enforcement agents. In addition, new federal and state laws have been aimed at particular areas of high-tech crimes.

Congress has treated computer-related crime as a distinct federal offense since the passage of the Counterfeit Access Device and Computer Fraud and Abuse Law in 1984.⁷⁹ The act protected classified U.S. defense and foreign relations information, financial institution and consumer reporting agency files, and access to computers operated for the government. The act was supplemented in 1996 by the National Information Infrastructure Protection Act (NIIPA), which significantly broadened the scope of the law.⁸⁰

Existing laws are sometimes inadequate to address the problem of cybercrime. Therefore new legislation has been drafted to protect the public from this new breed of criminal. Before October 30, 1998, when the Identity Theft and Assumption Deterrence Act of 1998 became law, there was no federal statute that made identity theft a crime. The Identity Theft and Assumption Deterrence Act accomplished four things:

- It made identity theft a separate crime against the individual whose identity was stolen and credit destroyed. Previously, victims had been defined solely by financial loss and often the emphasis was on banks and other financial institutions, rather than on individuals.
- It established the Federal Trade Commission (FTC) as the federal government's one central point of contact for reporting instances of identity theft by creating the Identity Theft Data Clearinghouse.
- It increased criminal penalties for identity theft and fraud. Specifically, the crime now carries a maximum penalty of 15 years imprisonment and substantial fines.
- It closed legal loopholes, which previously had made it a crime to produce or possess false identity documents, but *not* to steal another person's personal identifying information.⁸¹

Today, federal prosecutors are making substantial use of the statute and are actively prosecuting cases of identity theft. In addition, almost all states have by now passed laws related to identity theft.

In the wake of the 9/11 attacks, the NIIPA was amended by sections of the USA Patriot Act to make it easier to prosecute crimes by terrorists and other organized enemies against the nation's computer systems. Subsection 1030(a)(5)(A)(i) of the act criminalizes knowingly causing the transmission of a program, code, or command, and as a result, intentionally causing damage to a protected computer. This section applies regardless of whether the user had authorization to access the protected computer; company insiders and authorized users can be culpable for intentional damage to a protected computer. The act also prohibits intentional access without authorization that results in damage but does not require intent to damage; the attacker can merely be negligent or reckless.

International Treaties

Because cybercrime is essentially global, international cooperation is required for its control. The Convention on Cybercrime, ratified by the U.S. Senate in August 2006, was the first international treaty to address the definition and enforcement of cybercrime. Now signed by 46 nations, it focuses on improving investigative techniques and increasing cooperation among nations. The Convention includes a list of crimes that each signatory state must incorporate into their own law, including such cyber offenses as hacking, distribution of child pornography, and protection of intellectual property rights. It also allows law enforcement agencies new powers, including the ability to require that an Internet service provider monitor a person's online viewing

L04 Discuss efforts to control cybercrime.

and search choices in real time. The Convention also requires signatory states to cooperate whenever possible in the investigations and prosecution of cybercriminals. The vision is that a common legal framework will eliminate jurisdictional hurdles to facilitate the law enforcement of borderless cybercrimes.⁸²

Cybercrime Enforcement Agencies

To enforce these laws, federal, state, and local law enforcement agencies have put together a number of unified efforts to identify, control, and prosecute cybercrime. One approach is to create working groups that coordinate the activities of numerous agencies involved in investigating cybercrime. The International Mass-Marketing Fraud Working Group brings together representatives of numerous U.S. attorneys' offices, the FBI, the Secret Service, the Postal Inspection Service, the Federal Trade Commission, the Securities and Exchange Commission, Immigration and Customs Enforcement, and other law enforcement and regulatory agencies to share information about trends and patterns in Internet fraud schemes.⁸³

The New York/New Jersey Electronic Crimes Task Force (NYECTF) is a partnership between the U.S. Secret Service and a host of other public safety agencies and private corporations. The task force consists of more than 250 individual members representing federal, state, and local law enforcement, the private sector, and computer science specialists from 18 universities. Since 1995, the NYECTF has charged more than 1,000 individuals with electronic crime losses exceeding \$1 billion. It has trained more than 60,000 law enforcement personnel, prosecutors, and private industry representatives in cybercrime prevention. Its success has prompted similar electronic crime task forces to be set up in Boston, Miami, Charlotte, Chicago, Las Vegas, San Francisco, Los Angeles, and Washington, D.C.⁸⁴

On a broader scale, the National Cyber Investigative Joint Task Force (NCIJTF) consists of nearly two dozen federal intelligence, military, and law enforcement agencies that work along with local law enforcement agencies and international and private industry partners. The NCIJTF serves as the government's central hub for coordinating, integrating, and sharing information related to cyber threat investigations. It is tasked with identifying hackers and understanding their motivations and capabilities, disrupting criminal operations, and minimizing the consequences of intrusions. Rather than focusing on narrow or localized cybercrimes, the NCIJTF looks at the overall cyber landscape, attempting to counteract broad strategic shifts in cybercriminals' tactics and movements. It helps train local operatives, coordinate the sharing of intelligence across government agencies, and integrate the response to intrusions and investigations.⁸⁵

Another specialized agency that works with citizens who have been cybercrime victims, the Internet Crime Complaint Center, based in Fairmont, West Virginia, is run by the FBI and the National White Collar Crime Center. It brings together about 1,000 state and local law enforcement officials and regulators. Its goal is to analyze fraud-related complaints in order to find distinct patterns, develop information on particular cases, and send investigative packages to law enforcement authorities in the jurisdiction that appears likely to have the greatest investigative interest in the matter. The Internet Crime Complaint Center (IC³) receives nearly 300,000 complaints per year, which represent losses of close to \$800 million. They investigate auction fraud, nondelivery, and credit/debit card fraud, as well as nonfraudulent complaints, such as computer intrusions, spam/unsolicited email, and child pornography.⁸⁶ Law enforcement has made remarkable strides in dealing with identity theft as a crime problem over the last several years.

L05 Trace the evolution of organized crime.

Transnational Organized Crime

Transnational organized crime (TOC or transnational crime) is a form of organized crime operating across national borders. (See the accompanying Policies and Issues in Criminology feature for the history of organized crime.) It involves groups or networks of individuals working in more than one country to plan and execute illegal business

ventures. These criminal conspiracies involve ongoing criminal enterprise groups whose ultimate purpose is personal economic gain through illegitimate means. These groups do not hesitate to utilize systematic violence and corruption to get what they want and achieve their criminal goals: prostitution, pornography, gambling, and narcotics. The system may resemble a legitimate business run by an ambitious chief executive officer, his or her assistants, staff attorneys, and accountants, with thorough, efficient accounts receivable and complaint departments.⁸⁷ Cross-national gangs are often large criminal organizations, some with more than 20,000 members whose activities are bicoastal; the criminal activities of transnational gangs are global and have no borders.

This section briefly defines transnational organized crime, reviews its history, and discusses its economic effect and control.

Characteristics of Transnational Organized Crime

A precise description of the characteristics of transnational organized crime is difficult to formulate, but here are some of its general traits:⁸⁸

- Transnational organized crime is a conspiratorial activity, involving the coordination of numerous people in the planning and execution of illegal acts or in the pursuit of a legitimate objective by unlawful means (e.g., threatening a legitimate business to get a stake in it).
- An offense is transnational if:
 - It is committed in more than one state or nation.
 - It is committed in one state or nation but a substantial part of its preparation, planning, direction, or control takes place in another state or nation.
 - It is committed in one state or nation but involves an organized criminal group that engages in criminal activities in more than one state or nation.
 - It is committed in one state or nation but has substantial effects in another state or nation.⁸⁹
- Transnational organized crime involves continuous commitment by primary members, although individuals with specialized skills may be brought in as needed.
- Transnational organized crime is usually structured along hierarchical lines—a chieftain supported by close advisers, lower subordinates, and so on.
- Transnational organized crime has economic gain as its primary goal, although power and status may also be motivating factors. Economic gain is achieved through global supply of illegal goods and services, including drugs, sex slaves, arms, and pornography.
- In addition to providing illegal material such as narcotics, contemporary global syndicates engage in business crimes such as laundering illegal money through legitimate businesses, land fraud, and computer crime.
- Transnational criminal syndicates employ predatory tactics, such as intimidation, violence, and corruption.
- Transnational organized crime groups are quick and effective in controlling and disciplining their members, associates, and victims and will not hesitate to use lethal violence against those who flaunt organizational rules.



Roland Schlegel/EPA/Landov

Trafficking in humans can have deadly results. Here, on August 27, 2015, forensic experts investigate a truck in which 71 refugees were found dead on the autobahn A4 between Parndorf and Neusiedl, Austria. Europe is suffering a massive influx of refugees from the Middle East as fighting continues, and traffickers are looking to cash in on their desperation to emigrate to the West.

FACT OR FICTION?

Organized crime in the United States is a local commodity, controlled by five Mafia families in New York City and a few other allied groups in Chicago, Los Angeles, and Miami.

FICTION Traditional organized crime families are in decline, being replaced by transnational crime groups originating in Europe, Asia, and Latin and South America.

Policies and Issues in Criminology

ORIGINS OF ORGANIZED CRIME

While transnational gangs are a product of the IT age, organized crime has existed for more than 400 years. In the 1600s, London was terrorized by organized gangs that called themselves Hectors, Bugles, Dead Boys, and other colorful names. In the seventeenth and eighteenth centuries, English gang members wore distinctive belts and pins marked with serpents, animals, stars, and the like. The first mention of youth gangs in America occurred in the late 1780s, when prison reformers noted the presence of gangs of young people hanging out on Philadelphia's street corners. By the 1820s, New York's Bowery and Five Points districts, Boston's North End and Fort Hill, and the outlying Southwark and Moyamensing sections of Philadelphia were the locales of youth gangs with names like the Roach Guards, Chichesters, Plug Uglies, and Dead Rabbits.

At the turn of the twentieth century, La Mano Nera (the Black Hand), an offshoot of Sicilian criminal groups, established itself in northeastern urban centers. Gangsters demanded payments from local businessmen in return for "protection"; those who would not pay were beaten and their shops vandalized. Eventually the Black Hand merged with gangs of Italian heritage to form larger urban-based gangs and groups.

A turning point in the development of organized gangs occurred on January 16, 1919, when the

Eighteenth Amendment to the U.S. Constitution was ratified. The new amendment prohibited the sale, manufacture, and transportation of intoxicating liquors. Until then gangs had remained relatively small and local, but now the national market for controlled substances opened the door to riches. What emerged was a national syndicate, referred to as La Cosa Nostra or the Mafia, that was centrally coordinated and whose various component gangs worked cooperatively to settle disputes, dictate policy, and assign territory. Despite efforts at cooperation and control, numerous and bloody gang wars and individual vendettas were common.

The Mafia remains the largest organized crime group in the United States. Major families have a total membership of about 1,000 to 2,000 "made men," who have been inducted into organized crime families, and another 17,000 "associates," who are criminally involved with syndicate members. The families control crime in distinct geographic areas. New York City, the most important organized crime area, alone contains five families—the Gambino, Columbo (formerly Profaci), Lucchese, Bonanno, and Genovese families—named after their founding "godfathers." In contrast, Chicago contains a single mob organization called the "outfit," which also influences racketeering in such cities as Milwaukee, Kansas City, and Phoenix. The families are believed to be ruled by a "commission" made up of the heads of the five New York families and bosses from Detroit, Buffalo, Chicago, and Philadelphia, which settles personal problems and jurisdictional conflicts and

- Transnational crime depends heavily on the instruments of the IT age: the Internet, global communications, rapid global transportation systems, universal banking system, and global credit card and payment systems.
- Transnational organized crime groups do not include terror organizations, though there may be overlap. Some terror groups are involved in criminality to fund their political objectives, and some have morphed from politically motivated organizations to ones solely involved in for-profit criminal activity. Transnational criminal organizations may aid terror groups with transportation and communication.

L06 Discuss the activities of transnational organized crime.

Activities of Transnational Organized Crime

What are the main activities of transnational organized crime? The traditional sources of income are derived from providing illicit materials and using force to enter into and maximize profits in legitimate businesses. Most organized crime income comes from such activities as human trafficking, narcotics distribution, smuggling, and illegal gambling. Theft rings, Internet pornography, and cargo theft are other sources of income.

enforces rules that allow members to gain huge profits through the manufacture and sale of illegal goods and services.

Mafia in Decline

The American Mafia has been in decline. One reason: high-profile criminal prosecutions using up-to-date IT methods for surveillance and evidence collection. Chicago mob boss Frank Calabrese, Sr., was sentenced to life in prison in 2009 for his role in 18 gangland slayings dating back to 1970. His arrest—along with 13 others—meant that the Chicago mob does not have the power and influence it once had in the city. In another high-profile case, James “Whitey” Bulger was arrested after having been on the run for 16 years. Bulger, who once ran Boston’s feared Winter Hill Gang, was wanted for his role in 19 murders.

The Mafia leadership is aging. A number of the reigning family heads are quite old, in their 80s and older. A younger generation of mob leaders have stepped in to take control of the families, and they seem to lack the skill and leadership of the older bosses. The code of silence that protected Mafia leaders is now broken regularly by younger members who turn informer rather than face prison terms. When Joe Calabrese was on trial, his own son testified against him in court. In addition, active government enforcement policies have halved what the estimated mob membership was 25 years ago, and a number of the highest-ranking leaders have been imprisoned.

Traditional organized crime has also been hurt by changing values in U.S. society. European American neighborhoods, which were the locus of Mafia power, have been shrinking as families move to the suburbs. Organized crime groups lost their urban-centered political and social base of operations. In addition, success has hurt organized crime families: younger family members are better educated than their forebears and are equipped to seek their fortunes through legitimate enterprise. So while the traditional Mafia is still in business, its power is being replaced by transnational crime cartels. Traditional organized families had well-defined turf; transnational gangs respect no boundaries.

Critical Thinking

Can you think of parallels to the erosion of local crime families and their replacement by transnational groups? In other words, do changes in organized crime reflect changes in other social institutions?

Sources: Howard Abadinsky, *Organized Crime* (Belmont, CA: Wadsworth, 2012); FBI, “The Chicago Mafia: Down but Not Out,” June 27, 2011, www.fbi.gov/news/stories/2011/june/the-chicago-mafia/the-chicago-mafia (accessed 2015); Christopher Adamson, “Defensive Localism in White and Black: A Comparative History of European-American and African American Youth Gangs,” *Ethnic and Racial Studies* 23 (2000): 272–298; Donald Cressey, *Theft of the Nation* (New York: Harper & Row, 1969).

Because cross-national and transnational gangs are a product of the cyber age, members use cyberspace to communicate and promote their illicit activities. Gangs typically use the voice and text messaging capabilities of cell phones to conduct drug transactions and prearrange meetings with customers. Prepaid cell phones are used when conducting drug trafficking operations. Social networking sites, encrypted email, and instant messaging are commonly used by gang members to communicate with one another and with drug customers. Gang members use social networking sites such as YouTube and Facebook as well as personal web pages to communicate and boast about their gang membership and related activities. Some use the Internet to intimidate rival gang members and maintain websites to recruit new members. Gang members flash gang signs and wear gang colors in videos and photos posted on the Web. Sometimes, rivals “spar” on Internet message boards.⁹⁰

The Rise of Transnational Gangs

Traditional Eurocentric gangs are being replaced by transnational mega-gangs. Some, such as the Crips, Bloods, and MS-13, have expanded from local street gangs to

national mega-gangs with thousands of members. For example, the Sureños is an alliance of hundreds of individual Mexican American street gangs that originated in Southern California. Sureños gang members' main sources of income are retail-level distribution of cocaine, heroin, marijuana, and methamphetamine within prison systems and in the community as well as extortion of drug distributors on the streets. Some members have direct links to Mexican drug traffickers, brokering large drug transactions; they are also involved in other criminal activities such as assault, carjacking, home invasion, homicide, and robbery. While most members remain in Southern California cities, the gang has spread significantly and can be found throughout much of the United States.⁹¹

In addition to these homegrown gangs, international gangs based in Asia, Eastern Europe, North, South, and Latin America use the Internet and other IT devices to facilitate their operations across nations and continents. Emerging transnational crime syndicates are primarily located in nations whose governments are too weak to present effective opposition. If they believe that the government is poised to interfere with their illegal activities, they will carry out a terror campaign, killing police and other government officials to achieve their goals. Easier international travel, expanded world trade, and financial transactions that cross national borders have enabled them to branch out of local and regional crime to target international victims and develop criminal networks within more prosperous countries and regions.⁹² For example, Africa, a continent that has experienced political turmoil, has also seen the rise of transnational gangs. African criminal enterprises in Nigeria, Ghana, and Liberia have developed quickly since the 1980s due to the globalization of the world's economies and the great advances in communications technology. Nigerian criminal enterprises, primarily engaged in drug trafficking and financial frauds, are the most significant of these groups and operate in more than 80 countries. They are infamous for their email-based financial frauds, which cost the United States alone an estimated \$1 billion to \$2 billion each year.

Some of the most prominent transnational gang clusters are described here in some detail.

EASTERN EUROPEAN GANGS Eastern European gangs trace their origins to countries spanning the Baltics, the Balkans, Central/Eastern Europe, Russia, the Caucasus, and Central Asia. For example, Albanian organized crime activities in the United States include gambling, money laundering, drug trafficking, human smuggling, extortion, violent witness intimidation, robbery, attempted murder, and murder.⁹³ Organized groups prey upon women in the poorest areas of Europe—Romania, the Ukraine, Bosnia—and sell them into virtual sexual slavery. Many of these women are transported as prostitutes around the world, some finding themselves in the United States.

Balkan organized crime groups have recently expanded into more sophisticated crimes, including real estate fraud and cybercrimes. Take for instance Armenian Power (AP), an international organized crime group formed in the East Hollywood district of Los Angeles in the 1980s. In its heyday, the gang's 250-person membership consisted not only of those of Armenian descent but members from other countries within the former Soviet Union. Its members and associates carry out violent criminal acts, including murders, attempted murders, kidnappings, robberies, extortions, and witness intimidation and kidnapping. The government began to crack down on this group and eventually indicted 90 Armenian Power leaders, members, and associates, including the head man, Mher Darbinyan, aka "Hollywood Mike" and "Capone." Darbinyan was indicted for a bank fraud scheme that used middlemen and runners to deposit and cash hundreds of thousands of dollars in fraudulent checks drawn on the accounts of elderly bank customers and businesses. He also organized and operated a sophisticated debit card skimming scheme that involved the installation and use of skimmers to steal thousands of customers' debit card numbers and PIN codes. He was eventually sentenced to 32 years in prison; 87 other members have been convicted. The AP case shows how today's transnational crime groups rely more on

sophisticated cybercrime conspiracies than they do on the brute force of yesterday's organized criminals.⁹⁴

RUSSIAN TRANSNATIONAL CRIME GROUPS Since the collapse of the Soviet Union in 1991, criminal organizations in Russia and other former Soviet republics such as Ukraine have engaged in a variety of crimes: drugs and arms trafficking, stolen automobiles, trafficking in women and children, and money laundering.⁹⁵ No area of the world seems immune, especially not the United States. America is the land of opportunity for unloading criminal goods and laundering dirty money.

Russian criminals make extensive use of the state governmental apparatus to protect and promote their criminal activities. Most businesses in Russia—legal, quasi-legal, and illegal—must operate with the protection of a *krysha* (roof). The protection is often provided by police or security officials employed outside their “official” capacities for this purpose. In other cases, officials are “silent partners” in criminal enterprises that they, in turn, protect. Valuable properties are purchased through insider deals for much less than their true value and then resold for lucrative profits.

Criminals have been able to directly influence the state's domestic and foreign policy to promote the interests of organized crime, either by attaining public office themselves or by buying public officials. As a result of these activities, corruption and organized crime are globalized. Russian organized crime is active in Europe, Africa, Asia, and North and South America. Massive money laundering is now common, which allows Russian and foreign organized crime to flourish. In some cases, it is tied to terrorist funding. Russian criminals have become involved in killings for hire in Central and Western Europe, Israel, Canada, and the United States.

In the United States, with the exception of extortion and money laundering, Russians have had little or no involvement in some of the more traditional types of organized crime, such as drug trafficking, gambling, and loan sharking. However, thousands of Russian immigrants are believed to be involved in criminal activity, primarily in Russian enclaves in New York City.⁹⁶ Russian criminal groups are extensively engaged in a broad array of frauds and scams, including health care fraud, insurance scams, stock frauds, antiquities swindles, forgery, and fuel tax evasion schemes. Russians are believed to be the main purveyors of credit card fraud in the United States. Legitimate businesses, such as the movie business and the textile industry, have become targets of criminals from the former Soviet Union, and they are often used for money laundering and extortion.

LATIN AMERICAN AND MEXICAN DRUG CARTELS Transnational crime cartels operate freely in South American nations such as Peru and Colombia. Caribbean nations such as Jamaica, the Dominican Republic, and Haiti are home to drug and gun smuggling gangs. The money from illicit trade strengthens and enlarges the gangs, enabling them to increase their involvement in intraregional and transnational dealing in order to gain more money. Furthermore, drug trafficking has contributed to a sharp increase in the availability and usage of firearms.⁹⁷

However, while island groups flourish, it is the Mexican drug cartels that are now of greatest concern. These transnational gangs have become large-scale suppliers of narcotics, marijuana, and methamphetamine to the United States, and Mexico has become a drug-producing and transit country. In addition, an estimated 90 percent of cocaine entering the United States transits Mexico. Mexican drug gangs routinely use violence, and fighting for control of the border regions has affected U.S. citizens. Americans have been kidnapped, and Mexican drug cartel members have threatened to kill U.S. journalists covering drug violence in the border region. Although Mexican drug cartels, or drug trafficking organizations, have existed for quite some time, they have become more powerful since Colombia was able to crack down on the Cali and Medellín cartels in the 1990s. Mexican drug cartels now dominate the wholesale illicit drug market in the United States. As a result, Mexican cartels are the leading wholesale launderers of drug money from the United States. Mexican and Colombian

trafficking organizations annually smuggle an estimated \$25 billion in drug proceeds into Mexico for laundering.

At one time numerous drug cartels operated in Mexico, including the Gulf, Tijuana, Los Zetas, Sinaloa, Juárez, Millennium, Oaxaca, and Colima cartels. In recent years, new cartels have formed, some have become allies, and others were decimated by government crackdowns and rival gangs. Today the dominant gangs seem to be the Sinaloa, Jalisco New Generation, La Resistencia, and Knights Templar cartels. However, in a constantly shifting landscape of drug activity, this lineup could change instantly.

ASIAN TRANSNATIONAL CRIME GROUPS Asian-based transnational crime groups are also quite active in such areas as human trafficking, narcotics, and money laundering.⁹⁸ Chinese gangs are involved in importing heroin from the neighboring Golden Triangle area and distributing it throughout the country. They are also involved in gambling and prostitution, activities that had all but disappeared under Mao Zedong's Communist regime. The two leading organized crime problems in Cambodia are drug production/trafficking and human trafficking. Drug traffickers also use Cambodia as a transit country and traffic Cambodian women into Thailand for sexual activities. In Taiwan, the number one organized crime problem is *heijin*, the penetration of mobsters into the legitimate business sector and the political arena. Gangs are now heavily involved in the businesses of bid-rigging, waste disposal, construction, cable television networks, telecommunications, stock trading, and entertainment. Further, starting in the mid-1980s, many criminals have successfully run for public office in order to protect themselves from police crackdowns. Taiwan's gangs are involved in gambling, prostitution, loan sharking, debt collection, extortion, and gang violence; kidnapping for ransom is also a serious concern.

Among the best-known Asian crime groups are:

- *Yakuza*. Japanese criminal group. Often involved in multinational criminal activities, including human trafficking, gambling, prostitution, and undermining licit businesses.
- *Fuk Ching*. Chinese organized criminal group in the United States. They have been involved in smuggling, street violence, and human trafficking.
- *Triads*. Underground criminal societies based in Hong Kong. They control secret markets and bus routes and are often involved in money laundering and drug trafficking.
- *Heijin*. Taiwanese gangsters who are often executives in large corporations. They are often involved in white-collar crimes, such as illegal stock trading and bribery, and sometimes run for public office.
- *Jao Pho*. Organized crime group in Thailand. They are often involved in illegal political and business activity.
- *Red Wa*. Gangsters from Thailand. They are involved in manufacturing and trafficking methamphetamine.⁹⁹

Controlling Transnational Crime

Efforts to combat transnational organized crime are typically in the hands of federal agencies. One approach is to form international working groups to collect intelligence, share information, and plot unified strategies among member nations. The FBI belongs to several international working groups aimed at combating transnational gangs in various parts of the world. For example, to combat the influence and reach of Eurasian organized crime the FBI is involved in the following groups and activities:

- *Eurasian Organized Crime Working Group*. Established in 1994, it meets to discuss and jointly address the transnational aspects of Eurasian organized crime that impact member countries and the international community in general. The member

countries are Canada, Great Britain, Germany, France, Italy, Japan, the United States, and Russia.

- *Central European Working Group.* This group is part of a project that brings together the FBI and Central European law enforcement agencies to discuss cooperative investigative matters covering the broad spectrum of Eurasian organized crime. A principal concern is the growing presence of Russian and other Eurasian organized criminals in Central Europe and the United States. The initiative works on practical interaction between the participating agencies to establish lines of communication and working relationships, to develop strategies and tactics to address transnational organized crime matters impacting the region, and to identify potential common targets.
- *Southeast European Cooperative Initiative.* This is an international organization intended to coordinate police and customs regional actions for preventing and combating transborder crime. It is headquartered in Bucharest, Romania, and has 12 fully participating member countries. The United States has been 1 of 14 countries with observer status since 1998. The initiative's center serves as a clearinghouse for information and intelligence sharing, allowing the quick exchange of information in a professional and trustworthy environment. The initiative also supports specialized task forces for countering transborder crime such as the trafficking of people, drugs, and cars; smuggling; financial crimes; terrorism; and other serious transborder crimes.

ANTI-ORGANIZED CRIME LAWS Congress has passed a number of laws that have made it easier for agencies to bring transnational gangs to justice. One of the first measures aimed directly at organized crime was the Interstate and Foreign Travel or Transportation in Aid of Racketeering Enterprises Act (Travel Act).¹⁰⁰ The Travel Act prohibits travel in interstate commerce or use of interstate facilities with the intent to promote, manage, establish, carry on, or facilitate an unlawful activity; it also prohibits the actual or attempted engagement in these activities.

In 1970, Congress passed the Organized Crime Control Act. Title IX of the act, probably its most effective measure, is the **Racketeer Influenced and Corrupt Organizations Act (RICO)**.¹⁰¹ RICO did not create new categories of crimes but rather new categories of offenses in racketeering activity, which it defined as involvement in two or more acts prohibited by 24 existing federal and 8 state statutes. The offenses listed in RICO include state-defined crimes (such as murder, kidnapping, gambling, arson, robbery, bribery, extortion, and narcotics violations) and federally defined crimes (such as bribery, counterfeiting, transmission of gambling information, prostitution, and mail fraud). RICO is designed to limit patterns of organized criminal activity by prohibiting involvement in acts intended to do the following:

- Derive income from racketeering or the unlawful collection of debts and use or investment of such income
- Acquire through racketeering an interest in or control over any enterprise engaged in interstate or foreign commerce
- Conduct business through a pattern of racketeering
- Conspire to use racketeering as a means of making income, collecting loans, or conducting business

An individual convicted under RICO is subject to 20 years in prison and a \$25,000 fine. Additionally, the accused must forfeit to the U.S. government any interest in a business in violation of RICO. These penalties are much more potent than simple conviction and imprisonment.

Racketeer Influenced and Corrupt Organizations Act (RICO)

Federal legislation that enables prosecutors to bring additional criminal or civil charges against people whose multiple criminal acts constitute a conspiracy. RICO features monetary penalties that allow the government to confiscate all profits derived from criminal activities. Originally intended to be used against organized criminals, RICO has also been used against white-collar criminals.

Why Is It So Difficult to Eradicate Transnational Gangs?

While international cooperation is now common and law enforcement agencies are willing to work together to fight transnational gangs, these criminal organizations

Transnational crime is extremely difficult to control. Here, an Afghan man harvests a poppy field in the Khogyani district of Jalalabad, east of Kabul. When foreign troops arrived in Afghanistan in 2001, one of their goals was to stem drug production. Instead, they have concentrated on fighting insurgents and have often been accused of turning a blind eye to the poppy fields. Afghanistan is now the leading provider of poppy, the basic ingredient for heroin. Controlling transnational crimes in places such as Afghanistan is all but impossible.



CHECKPOINTS

Transnational organized crime (TOC or transnational crime) is a form of organized crime operating across national borders.

Cross-national and transnational gang members use cell phones and the Internet to communicate and promote their illicit activities.

Transnational organized crime is a conspiratorial activity, involving the coordination of numerous people in the planning and execution of illegal acts or in the pursuit of a legitimate objective by unlawful means.

Most organized crime income comes from such activities as human trafficking, narcotics distribution, smuggling, illegal gambling, theft rings, Internet pornography, and cargo theft.

Efforts to combat transnational organized crime are typically in the hands of federal agencies.

One approach is to form international working groups to collect intelligence, share information, and plot unified strategies among member nations.

While international cooperation is now common and law enforcement agencies are willing to work together to fight transnational gangs, even when a gang can be taken out it is soon replaced as long as money can be made.

Adding to control problems is the fact that the drug trade is an important source of foreign revenue.

are extremely hard to eradicate. The gangs are ready to use violence and well equipped to carry out threats. Take for instance Los Zetas, whose core members are former members of the Mexican military's elite Special Air Mobile Force Group (Grupo Aeromovil de Fuerzas Especiales, or GAFES). Military trained, Los Zetas members are able to carry out complex operations and use sophisticated weaponry.¹⁰² Los Zetas began as enforcers for the Gulf cartel's regional domination but are now their rivals and considered the most powerful Mexican transnational gang. Their base is Nuevo Laredo, but the criminal organization's sphere of influence extends across Mexico and deep into Central America. Unlike most gangs, which obtain most of their income from narcotics, the Los Zetas cartel earns about half its income trafficking in arms, kidnapping, and competing for control of trafficking routes along the eastern half of the U.S.-Mexico border. The cartel is considered Mexico's most brutal.

Adding to control problems is the fact that the drug trade is an important source of foreign revenue, and destroying the drug trade undermines the economies of third-world nations. Even if the government of one nation were willing to cooperate in vigorous drug suppression efforts, suppliers in other nations, eager to cash in on the sellers' market, would be encouraged to turn more acreage over to coca or poppy production. Today, almost every Caribbean country is involved with narco-trafficking, and illicit drug shipments in the region are worth more money than the top five legitimate exports combined. Drug gangs are able to corrupt the political structure and destabilize countries. Drug addiction and violent crime are now common in Jamaica, Puerto Rico, and even small islands like St. Kitts. The corruption of the police and other security forces has reached a crisis point, where an officer can earn the equivalent of half a year's salary by simply looking the other way on a drug deal.¹⁰³ There are also indications that the drug syndicates may be planting a higher yield variety of coca and improving refining techniques to replace crops lost to government crackdowns.

The United States has little influence in some key drug-producing areas such as Taliban-held Afghanistan and Myanmar (formerly Burma). War and terrorism also may make gang control strategies problematic. After the United States toppled Afghanistan's Taliban government, the remnants began to grow and sell poppy to support their insurgency; Afghanistan now supplies 90 percent of the world's opium.¹⁰⁴ And while the Colombian guerrillas may not be interested in joining or colluding with crime cartels, they finance their war against the government by aiding drug traffickers and "taxing" crops and sales. Considering these problems, it is not surprising that transnational gangs continue to flourish.

Thinking Like a Criminologist

The Ethics of Monitoring Suspects

The president's national security advisor approaches you with a problem. It seems that a tracking device has been developed that can be implanted under the skin that will allow people to be constantly monitored. Implanted at birth, the data surveillance device could potentially cover *everyone*, with a record of every transaction and activity they engage in entered into databases monitored by powerful search engines that would keep them under constant surveillance. The surveillance device would enable the government to keep tabs on their whereabouts as well as monitoring biological activities such as brain waves, heart rate, and so on. The benefits are immense. Once a person becomes suspect in a crime or is believed to be part of a terrorist cell, they can be easily monitored from a distance without danger to any government agent. They cannot hide or escape detection. Physical readings could be made to determine if they are under stress, using banned substances, and so on.

To research the issue, you begin by reading what the American Civil Liberties Union has to say: "The United States is at risk of turning into a full-fledged surveillance society. The tremendous explosion in surveillance-enabling technologies, combined with the ongoing weakening in legal restraints that protect our privacy mean that we are drifting toward a surveillance society. The good news is that it can be stopped. Unfortunately, right now the big picture is grim."

Writing Assignment

The director wants you to write a paper for the NSA expressing your opinion on this device. Address whether it is worthwhile, considering the threats faced by America from terrorists and criminals. Or, as the ACLU suggests, would it be unethical because it violates the personal privacy and freedom of people before they have broken any law?

SUMMARY

L01 Discuss the concept of cybercrime and why it has become important.

Cybercrime is a relatively new breed of offenses that involves the theft and/or destruction of information, resources, or funds utilizing computers, computer networks, and the Internet. Cybercrime presents a challenge for the justice system because it is rapidly evolving, it is difficult to detect through traditional law enforcement channels, and its control demands that agents of the justice system develop technical skills that match those of the perpetrators. Cybercrime has grown because information technology (IT) has become part of daily life in industrialized societies.

L02 Distinguish among cybertheft, cybervandalism, and cyberterrorism.

Some cybercrimes use modern technology to accumulate goods and services (cybertheft). Cybervandalism involves malicious attacks aimed at disrupting, defacing, and destroying technology that the attackers find offensive. Cyberterrorism is aimed at undermining the social, economic, and political system of an enemy nation by destroying its electronic infrastructure and disrupting its economy.

L03 Describe the various types of cybercrimes, such as computer frauds, illegal copyright infringement, and identity theft.

There are a number of methods that hackers use to commit cybercrimes. *Warez* refers to groups of individuals who work together to illegally obtain software and then "crack" or "rip" its copyright protections before posting it on the Internet for other members of the group to use. Another type of illegal copyright infringement involves file-sharing programs that allow Internet users to download music and other copyrighted material without

paying the artists and record producers their rightful royalties. Identity theft occurs when a person uses the Internet to steal someone's identity and/or impersonate the victim to open a new credit card account or conduct some other financial transaction. Phishing involves the creation of false emails and websites that look legitimate but are designed to gain illegal access to a victim's personal information.

L04 Discuss efforts to control cybercrime.

The growth of cybercrime and its cost to the economy has created the need for new laws and enforcement processes specifically aimed at controlling its emerging formulations. Congress has treated computer-related crime as a distinct federal offense since passage of the Counterfeit Access Device and Computer Fraud and Abuse Law in 1984. Existing laws sometimes are inadequate to address the problem of cybercrime. Therefore new legislation has been drafted to protect the public from this new breed of criminal. Specialized enforcement agencies have been created to crack down on cybercriminals.

L05 Trace the evolution of organized crime.

Organized criminals were traditionally white ethnics, but today other groups have become involved in organized crime activities. The old-line "families" are now more likely to use their criminal wealth and power to buy into legitimate businesses. The most common view of organized crime today is an ethnically diverse group of competing gangs dedicated to extortion or to providing illegal goods and services. Efforts to control organized crime have been stepped up by the federal government, which has used antiracketeering statutes to arrest syndicate leaders.

L06 Discuss the activities of transnational organized crime.

With the aid of the Internet and instant communications, transnational groups are operating on a global scale to traffic drugs and people, launder money, and sell arms. Eastern European crime families are active abroad and in the United States. Russian organized crime has become a major problem for law enforcement agencies. Mexican and Latin American groups are quite active in the drug trade. Asian crime families are involved in smuggling and other illegal activities.

Key Terms

cybercrime 454
transnational organized
crime 454
cybertheft 455
cybervandalism 455
cyberwar/cyberterrorism
455
warez 456

salami slice fraud 456
ATM skimming 457
denial-of-service attack
(DoS) 460
pump and dump 461
cyber smear 461
identity theft 461
phishing 461

spear-phishing 461
etailing fraud 462
computer virus 464
malware 464
computer worms 464
Trojan horse 464
logic bomb 464
spam 464

website defacement 464
cyberstalking 465
cyberbullying 466
cyberspying 466
cyberespionage 467
Racketeer Influenced and
Corrupt Organization
Act (RICO) 479

Critical Thinking Questions

1. Which theories of criminal behavior best explain the actions of cybercriminals, and which ones do you believe fail to explain cybercrime?
2. How would you punish a web page defacer who placed an antiwar message on a government site? Prison? Fine?
3. What guidelines would you recommend for the use of IT in law enforcement?
4. Are we creating a "Big Brother" society and is the loss of personal privacy worth the price of safety?
5. What can be done to reduce the threat of transnational organized crime?