

CRIMINAL JUSTICE, 3/e

© 2005

Jay S. Albanese

ISBN **0-205-42202-0**

(Please use above number to order your exam copy.)

Visit www.ablongman.com/relocator to contact your local Allyn & Bacon/Longman representative.

s a m p l e c h a p t e r

The pages of this Sample Chapter may have
slight variations in final published form.

Allyn & Bacon
75 Arlington St., Suite 300
Boston, MA 02116
www.ablongman.com



Economic and Political Crime

What Is Meant by Economic and Political Crimes?

How Can White-Collar Crimes Be Defined?

- Types of White-Collar Theft
- Crimes against Public Administration
- Corporate Crimes
- Trends in White-Collar Crime

Why Is Computer Crime a Growing Threat?

- Types of Computer Crimes
- Consequences of Computer Crime

How Does Organized Crime Operate?

- A Typology of Organized Crime
- Organized Crime Offenders
- National and International Aspects of Organized Crime

What Are the Impacts of Terrorism and Hate Crimes?

- Terrorism and Hate Crime Trends
- How Terrorism and Hate Crimes Merge

THAT'S A FACT

Perspectives on Terrorism

MEDIA AND CRIMINAL JUSTICE

A Civil Action

CRITICAL THINKING EXERCISES

- Is the Internet an Avenue for Terrorists?
- Should There Be Limits on Controlling Pollution?





Learning Objectives

Identify and define categories of economic and political crime.

Explain the differences among types of white-collar crimes and their main characteristics.

Describe patterns and trace trends in economic and political crimes.

Analyze types of computer crime and their impacts on society today.

Compare and contrast forms of organized crime and their perpetrators.

Give examples of challenges in transnational crime prevention and law enforcement.

Explain the concepts of terrorism and hate crime and their interrelationship.

Whereas most street crimes are

either random or involve very little planning, sophisticated crimes require planning or organization to succeed. Most street crimes take only a few minutes or even seconds to accomplish. Economic and political crimes often take days, weeks, and sometimes months to plan and carry out. Speculation was growing that Enron, one of the world's largest companies, was facing serious financial troubles in its cable and energy businesses. Its stock price had plunged by \$20 per share. But CEO Jeffrey Skilling told securities analysts in 2001 he was "highly confident" about the company's condition. "I know this is a bad stock market, but Enron's in good shape," he said. Skilling was indicted in 2004, charged that he knew that Enron was

failing and that jobs were going to be cut. The indictment alleged that Enron failed to meet its budget targets and was able to appear successful only through fraud. Skilling and former Enron chief accounting officer Richard Causey were charged with widespread financial scheming and trading stock on non-public “insider” information, allegedly pocketing \$200 million from insider stock sales. Skilling unexpectedly resigned as Enron CEO in 2001, but sold 500,000 company shares of stock a month later for a \$15.6 million gain. Skilling was the highest level executive of Enron to be charged in a scandal that ended in the convictions of several executives and resulted in prison sentences and millions of dollars in fines. All cases involved fraudulent accounting tactics to hide Enron’s weak financial condition, so that executives could benefit personally before driving the company into bankruptcy, costing employees their jobs and investors their money.

In another Wall Street case, home decorating queen and highly successful businesswoman Martha Stewart went on trial in 2004 on criminal charges she sold 4,000 shares of biotechnology company ImClone Systems, which was run by her friend Samuel Waksal. The sale came one day before ImClone announced that health regulators had rejected a key new drug application it had developed, sending its stock price plunging. Waksal is serving a seven-year prison term after pleading guilty to securities fraud over his family’s sale of the ImClone shares. Stewart was convicted of making false statements to investigators about the sale.

Consider also the case of Royal Caribbean Cruises, the second-largest passenger cruise line in the world. The company had promoted itself as an environmentally responsible company, but pled guilty to twenty-one felony charges for dumping waste oil and hazardous chemicals at sea and then lying about it to the U.S. Coast Guard. Royal Caribbean admitted it routinely dumped oil from its ships a year earlier, but continued the conduct while under court supervision. The investigation found that some of the company’s ships had no oil-contaminated wastewater, when these ships produce 100,000 gallons of wastewater annually. Hazardous chemicals from photo-processing equipment, dry cleaning shops, and printing presses also were dumped at sea, in ports, and in environmentally sensitive areas. The company was fined a record \$18 million in addition to \$9 million in fines it was assessed a year earlier. Federal investigators said Royal Caribbean crew members wore buttons declaring “Save the Waves” at the same time the company was engaged in illegal dumping.¹

Consider the similarities between the Wall Street and Royal Caribbean cases and another crime that occurred more than a half century earlier. The famous gangster Al Capone was widely believed to be involved in illegal gambling and bootlegging, but no one was able to prove it. Then the IRS examined his bank accounts and spending habits in Miami and Chicago and found that Capone had spent \$7,000 for suits, \$1,500 per week for hotel bills, \$40,000 for a house on Palm Island, \$39,000 on telephone calls, and \$20,000 for silverware. This spending pattern suggested that he earned \$165,000 per year. The IRS asked Capone to show how he lawfully earned this amount

CRIMES OF THE FUTURE

of money. Capone could not do so and was tried and convicted for failure to pay income taxes on \$1 million of illegal income.²

In these cases it can be seen that planning and organization were central to the commission of the crimes charged, and that the crimes can be ongoing in nature. Sophisticated economic and political crimes are characterized by such planning.

These crimes will reach new levels in the coming years. An aging population no longer suited to committing street crimes, more service industry jobs with access to cash and personal information, computers in most homes and workplaces, the ease of international travel and trade, and Internet communication for terrorists and hate groups—this combination of circumstances will promote new forms of white-collar, organized, and computer crime and will promote terrorism and hate crimes. Those who will exploit the opportunities and technologies of the era will be clever.

Economic and political crimes are the most serious crimes occurring today, and they are the subject of this chapter. The following sections highlight several types of sophisticated crimes and their impact on our lives.

CONSPIRACY

■ conspiracy

Agreement between two or more persons to commit a crime or to carry out a legal act in an illegal manner.

■ white-collar crimes

Crimes of fraud, crimes against public administration, and regulatory offenses that are usually carried out during the course of a legitimate occupation.

■ crimes of fraud

Embezzlement, extortion, forgery, and fraud.

■ crimes against public administration

Attempts to impede government processes through bribery, obstruction of justice, official misconduct, or perjury.

■ regulatory offenses

Attempts to circumvent regulations designed to ensure fairness and safety in the conduct of business; include administrative, environmental, labor, and manufacturing violations as well as unfair trade practices.

What Is Meant by Economic and Political Crimes?

Economic and political crimes include white-collar crime, organized crime, computer crime, international and domestic terrorism, and some forms of hate crimes. The common behaviors that underlie these crimes link them together. The criminal law punishes the kind of criminal planning that underlies sophisticated crimes such as **conspiracy**. Conspiracy takes place when two or more persons agree to commit a crime or to carry out a legal act in an illegal manner. Conspiracy, then, is essentially *preparation* or planning to commit a crime. The importance of making conspiracy a crime can be seen in virtually every case of white-collar, computer, and organized crime, in which authorities can punish the *planning* activities of sophisticated criminals, thereby thwarting their criminal designs.

White-collar crimes are crimes that are usually carried out during the course of a legitimate occupation. In place of the force or stealth that is inherent in violent and property crimes, white-collar crimes employ deceit in an effort to trick an unsuspecting victim. White-collar crimes are of three types: crimes of fraud, crimes against public administration, and regulatory offenses.³ **Crimes of fraud** have money as their object and include embezzlement, extortion, forgery, and fraud. **Crimes against public administration** attempt to impede government processes. These include bribery, obstruction of justice, official misconduct, and perjury. **Regulatory offenses** are violations that circumvent measures designed to protect public health, safety, or welfare in business, industry, and government. It can be seen that *white-collar crime* is a generic term that encompasses several specific types of crimes.

How Can White-Collar Crimes Be Defined?

White-collar crime goes beyond the crimes committed by business and professional people who often wear jackets, ties, and white shirts to work. It is easy to distinguish a mugging from an embezzlement, but what about the difference between simple theft and fraud? Or between assault and an injury caused by a defective product? The distinctions between white-collar and traditional street crimes are not always clear. These two categories of offenses are not distinguishable by the amount of harm they cause, because frauds or unsafe products can cause much more injury and harm than any number of street crimes. Nor are they distinguishable by the level of violence involved. Many street crimes, such as larceny and burglary, involve no personal confrontation, but conspiracy, extortion, or food and drug manufacturing violations can involve threats, injury, and even death. The distinctions between white-collar crime and more traditional forms of crime therefore do not lie in the nature of the victim, or in the amount of violence, or in the extent of injury. Instead, white-collar crime is distinguishable by the manner in which it is carried out, given available opportunities. The opportunity to commit such crimes is often determined by one's position in society. One cannot embezzle funds without first holding a position of financial trust, nor can one commit regulatory offenses without holding a particular position in business or industry. Thus, *access* to financial or governmental or institutional resources provides the *opportunity* to commit white-collar offenses.

Street crimes are characterized by the use of *force or stealth*, which is required for homicide, rape, robbery, assault, burglary, larceny, or arson. In contrast, white-collar crimes are characterized by planning and deceit. *Planning and deceit* are required for successful conspiracy, fraud, extortion, embezzlement, forgery, or regulatory offenses. Thus, white-collar crimes can be defined as:

*planned illegal acts of deception committed by an individual or organization, usually during the course of legitimate occupational activity by persons of high or respectable social status, for personal or organizational gain that violates fiduciary responsibility or public trust.*⁴

This definition highlights several facts about white-collar crime:

- It can be committed by an individual or by an organization or group of individuals.
- Deception, trickery, or fraud lies at the heart of white-collar crime.
- Most white-collar crimes emanate from otherwise legitimate occupational activity in which access to money or information makes possible the misuse of one or both of these resources.
- White-collar offenses sometimes lie on the border between illegal and unethical behavior, where what a company does may cause

**WHITE-COLLAR
CRIME**

**ROLE OF
PLANNING
AND DECEIT**

harm or even death without actually violating the criminal law. Many unethical offenses are adjudicated in civil proceedings that determine compensation, rather than in criminal court, which determines guilt.

Types of White-Collar Theft

Table 5.1 shows a typology of white-collar crimes. As the table illustrates, white-collar crimes can be divided into three groups: theft, offenses against public administration, and regulatory offenses. White-collar thefts include embezzlement, extortion, forgery, and fraud. **Embezzlement** is the purposeful misappropriation of property entrusted to one’s care, custody, or control to which one is not entitled. In some states this crime is called “misapplication of property” and is included under theft as a type of larceny. The essential element of embezzlement is violation of fiduciary (or financial) trust. An example is seen in the case of the former chief financial officer of Day-Lee Foods in California, who was convicted of stealing \$100 million in company funds by manipulating company accounts over a period of seven years.⁵ Embezzlement is usually punished on the basis of how much money or property is misappropriated.

Extortion also involves theft, but it is accomplished in a different manner. It consists of purposely obtaining property from another person with that person’s consent, when that consent is induced through wrongful use of force or threat of force or under the guise of official authority. Many states classify extortion as a type of larceny or theft. Extortion is sometimes called blackmail, as in the case of Sol Wachtler, chief judge of the New York State Court of Appeals, who was charged with telling his former lover that he would sell sexually explicit photos of her and her new boyfriend if she did not give him money.⁶ The word *blackmail* is derived from European terms for money or payment (e.g., French *maille*, Gaelic *mal*, German *Mahl*). The “black” is believed to reflect the illegal nature of the payments and also may refer to the metal in which the payment historically was made. Copper or other base metal was usually used, rather than silver (a “white” metal). With

the advent of paper currency, metal coins are now infrequently used as a form of payment, but the term *blackmail* continues to be used today.

A person who falsely makes or alters an official document with intent to defraud commits the crime of **forgery**. The penalty for forgery is often based on the type of document that is forged. For example, forging passports or currency usually carries a higher penalty. Forgery also includes other offenses that are sometimes defined separately under state law. Counterfeiting money, criminal possession of forged documents, and falsifying business records are all variations of the crime of forgery. Federal offi-

■ embezzlement

The purposeful misappropriation of property entrusted to one’s care, custody, or control to which one is not entitled.

EMBEZZLEMENT AND EXTORTION

■ extortion

Purposely obtaining property from another person without consent through wrongful use of force or fear or under the guise of official authority.

FORGERY

■ forgery

Falsely making or altering an official document with the intent to defraud.

TABLE 5.1 A Typology of White-Collar Crime

CRIMES OF THEFT	CRIMES AGAINST PUBLIC ADMINISTRATION	REGULATORY OFFENSES
Embezzlement	Bribery	Administrative violations
Extortion	Obstruction of justice	Environmental violations
Forgery	Official misconduct	Labor violations
Fraud	Perjury	Manufacturing violations
		Unfair trade practices

SOURCE: *White-collar Crime in America* by Albanese, JAY, © 1995. Reprinted by permission of Prentice-Hall, Inc., Upper Saddle River, NJ.

cials began an investigation in 2000 when counterfeit law enforcement credentials were found to be available for purchase on the Internet. Undercover investigators were able to enter secure areas of airports and government buildings with the false identification.⁷

Another type of white-collar theft is **fraud**, or purposely obtaining the property of another person through deception. Fraud is at the heart of the concept of white-collar crime. Together with conspiracy, it forms the basis for many organized illegal acts. In many states bankruptcy fraud, false advertising, issuing a bad check, criminal impersonation, and theft of services are regarded as specific types of fraud. Fraud thus involves larceny by trickery or deceit. A common form of fraud is telemarketing scams. In a typical case, a New Jersey company used a 900 number to charge people up to \$28 per call for responding to mail announcing that they had won a prize—which turned out to be worthless jewelry.⁸ In a well-known case, American Family Publishers agreed to pay \$1.25 million to thirty-two states over allegations of deceptive sales practices. This company sent more than 200 million mailings annually, using the names of well-known celebrities Ed McMahon and Dick Clark, to tell each recipient that he or she was one of a very small number of winners. The mailings suggested that if recipients ordered magazine subscriptions, their chances of winning a multimillion-dollar prize would be enhanced. The company agreed to make it clearer in future mailings that no purchase was necessary to enter or win the sweepstakes prize. This settlement was similar to one reached between Publishers Clearing House and fourteen states a few years earlier.⁹ Although money is not obtained by theft in these cases, deceptive practices can trick a person into believing they are buying a chance at a million dollars through a magazine order. Obtaining money through deception is the essence of fraud.



Forgery is the alteration of an official document with intent to defraud, and knowingly buying or selling forged documents also are criminal acts. What “documents” typically are found in forgery cases? What characteristics of forgery make it a white-collar crime? What are some other types of white-collar theft?

Crimes against Public Administration

Crimes against public administration involve misconduct by government officials and by individuals attempting to disrupt or corrupt government processes. The crimes in this category include bribery, obstruction of justice, official misconduct, and perjury. **Bribery** involves the voluntary giving or receiving of anything of value with the intent to influence the action of a public official. The more important the official act to be performed is, the more serious the penalty. For example, bribery of a judge in a criminal case carries a significant penalty. Bribery law works two ways: One can be convicted of bribery for offering the corrupt payment as well as for receiving it. In South Carolina, for example, fifteen legislators and six lobbyists were among those convicted after the FBI videotaped legislators taking cash from

FRAUD

■ fraud

Purposely obtaining the property of another person through deception.

BRIBERY

■ bribery

Voluntary giving or receiving anything of value with the intent of influencing the action of a public official.

OBSTRUCTION**obstruction of justice**

Intentionally preventing a public servant from lawfully performing an official function.

MISCONDUCT**official misconduct**

The unauthorized exercise of an official function by a public official with intent to benefit or injure another.

PERJURY**perjury**

Making a false statement under oath in an official proceeding.

corporate crimes

Dangerous or unjust actions in the conduct of business prompted by the desire for profits. Same as *regulatory offenses*.

ADMINISTRATIVE OFFENSES

lobbyists in exchange for their votes.¹⁰ Seven Arizona legislators were charged in a similar bribery scandal.¹¹

Intentionally preventing a public servant from lawfully performing an official function is **obstruction of justice**. In the cover-up of the 1972 burglary of the Democratic party headquarters in the Watergate complex, for example, members of the White House staff refused to cooperate with investigations of alleged wrongdoing, and some were ultimately convicted of purposely concealing relevant information, which is obstruction of justice.¹² In 1993 three New York State troopers confessed to falsifying fingerprints in more than thirty criminal cases over a period of nine years in order to “solve” cases with adulterated evidence.¹³ Lying about this evidence in court was obstruction of justice.

Official misconduct is a public official’s unauthorized exercise of an official function with intent to benefit or injure another. Also, a person who uses an elected office for personal gain is guilty of official misconduct. Such misconduct can result from an act of omission (failure to perform legal duties) or commission (exercising powers in an unauthorized manner). People who use their public office to “fix” tickets, obtain permits without payment, or solicit sex are committing official misconduct. In 2000 a municipal judge in Cleveland was accused of soliciting payments from defendants to influence his decisions, which is a form of official misconduct.¹⁴

When someone makes a false statement under oath in an official proceeding, he or she is guilty of **perjury** or false swearing. The punishment for perjury is usually based on the nature of the proceeding. Perjury during a trial or grand jury proceeding is considered more serious than false swearing on an affidavit. John Poindexter, former national security advisor to President Reagan, was convicted of perjury when he was shown to have lied to Congress as part of the cover-up in the Iran–Contra affair.¹⁵ In 1999 inside information provided by a former officer in the Los Angeles Police Department resulted in the dismissal of several cases due to confirmed instances of false testimony and planted evidence.¹⁶

Corporate Crimes

The third category of white-collar crimes is **corporate crimes**, also called regulatory offenses. The laws governing these offenses are designed to ensure fairness and safety in the conduct of business so that the desire for profits does not lead to dangerous or unjust actions. There are hundreds of types of regulatory offenses, but they can be grouped into five different categories: administrative, environmental, labor, and manufacturing violations, and unfair trade practices.

Administrative offenses involve the failure to comply with court orders or agency requirements. Failures to keep adequate records, submit compliance reports, acquire a valid permit, and the like are against the law where these procedures are required. For example, Equifax, a leading credit-reporting agency, settled a case brought by eighteen states alleging that it was issuing inaccurate credit reports. The company agreed to make credit reports easier to read, to explain to consumers how a credit rating is derived,

and to resolve disputed reports within thirty days. Another credit-reporting agency, TRW, settled a similar case brought by nineteen states.¹⁷ In the year 2000, Bayer agreed to pay \$1 million over an inaccurate claim that nearly all adults could prevent heart attacks with aspirin.¹⁸ In 2003, the first conviction occurred in the Enron scandal, which involved massive fraud and misrepresentation in an energy-trading company.¹⁹

Environmental violations include emissions or dumping in violation of legal standards. Discharges of harmful substances into the air or water without a permit, failure to treat waste adequately before disposal, and deposit of hazardous waste in a landfill are examples of environmental violations. A Michigan man was sentenced to three years in prison and to pay restitution for his role in abandoning 70 drums of hazardous waste in an empty field.²⁰

Labor violations can take several forms, including discriminatory hiring practices, exposure of employees to harm in the workplace environment, and unfair treatment of employees. Examples of unfair treatment include firing without cause, refusing employment, and ignoring complaints of sexual harassment. Imperial Food Products officials were charged in 1992 with twenty-five counts of involuntary manslaughter for locked exits and other safety violations that resulted in the deaths of twenty-five workers in a fire at Imperial's chicken-processing plant in Hamlet, North Carolina.²¹ A Boston contractor was fined by the Occupational Safety and Health Administration for repeated safety violations after a worker fell fifteen feet into a pit and was killed.²²

The manufacture of unsafe products is the essence of the manufacturing violations category. Electric shock hazards, fire hazards, and lack of adequate labeling or directions on products are examples of such violations. In one of the largest product liability cases in U.S. history the manufacturer of the diet drugs Redux and Pondimin agreed to pay \$3.75 billion to thousands of people who suffered, or might suffer in the future, from heart valve damage linked to the drugs. Two members of the Pilgrim family of Mississippi received prison sentences for selling syrup and honey products that were labeled as pure but were not made from pure ingredients.²³

Unfair trade practices prevent fair competition in the marketplace. Monopolization, price discrimination, price-fixing, and bid rigging are examples of unfair trade practices. In one case the state of Florida filed a lawsuit against three manufacturers of infant formula, claiming that they had conspired to raise the price of baby formula. The state pointed out that formula prices had risen 155 percent, whereas the price of milk, the primary ingredient, had risen only 36 percent over the same period.²⁴ Toys R Us and two other toy makers agreed to pay \$50 million to settle a multistate lawsuit claiming that they prevented other toy makers from selling popular toys to discount stores. The case arose from a complaint by the FTC that Toys R Us illegally used its size

ENVIRONMENTAL VIOLATIONS

LABOR VIOLATIONS

UNFAIR TRADE PRACTICES

In this photograph, what type of regulatory offense has been committed by a corporation? What other types of regulatory offenses are involved in corporate crimes? Do you think corporate crimes are potentially as harmful as violent and property crimes? Why or why not? What accounts for continuing increases in white-collar crime in the United States?



A CIVIL ACTION

Media and Criminal Justice

In the 1999 hit movie *A Civil Action*, the viewer is presented with a familiar stereotype of the civil lawyer: the arrogant, money-hungry, egotistical ambulance chaser. For the dynamic Jan Schlichtmann, winning a case is only about making money, not about procuring justice. The viewer is surprised, then, when Schlichtmann travels to Woburn, Massachusetts, to visit a group of parents who have lost children to leukemia. As the Woburn residents began to recognize the extraordinarily high rate of cancer in their community, significant toxic pollutants were found in two of the town's water wells.

Based on the book *A Civil Action* by Jonathan Harr, the film provides an excellent account of the real 1970s civil case against Beatrice Foods and W. R. Grace. In the movie we see a tannery foreman explaining that the process by which animal hides are cured involves pouring chemicals over the leather. Questions remain as to whether the chemical spillage from the process is responsible for the toxins in the wells and to what extent the pollutants were spread knowingly or intentionally. Because the alleged environmental violations have been blamed for the illness and deaths of many Woburn residents, Schlichtmann has the responsibility of proving specific cause and effect in relation to the damages he is claiming.

Perhaps the most interesting aspect of the story is how the case humanizes the showboat lawyer Schlichtmann. He is

clearly out for profit when he takes the case, but as he is faced with the suffering of the parents of Woburn's leukemia victims, his motive becomes more about justice than money. It is a position that will cost him the case: In his search for truth and justice, he turns down a \$20 million offer from Grace and a \$4 million offer from Beatrice. (The jury later would award \$8 million from Grace, allocated almost exclusively for toxic cleanup, and would absolve Beatrice of liability.) For the parents the civil action was obviously never about the money; but for Schlichtmann, the eye-opening experience leaves his prestigious law firm bankrupt.

Is it possible that corporations are aware of their regulatory crimes but determine that it is more financially advantageous to pay damages than to fix the problem? Should there be a cap on how much injured parties can recover from regulatory crimes? Who ultimately pays for the damages that corporations must remit if they lose in a civil action brought against them?



and domination of the toy market to force toy makers to supply toys to them and not to discount stores. In this way, Toys R Us was alleged to have unfairly reduced its competition in the toy market and to have artificially raised prices.²⁵

As the offense categories for corporate crimes illustrate, regulations are designed to protect the public from unscrupulous or dangerous business practices. This type of white-collar crime is based on deviations from legitimate business activity. Penalties for violating regulations sometimes involve criminal sanctions; thus, regulatory offenses are part of the criminal law.

Trends in White-Collar Crime

An important question is whether white-collar crime is increasing or decreasing. An answer is not readily available, because there are no regularly collected data for white-collar crimes as there are for street crimes. Victimization surveys count only rape, robbery, assault, burglary, larceny, and

TABLE 5.2 Arrests for White-Collar Crimes (Number and Rate per 100,000 Population)

OFFENSES	1970	1980	1995	2001	PERCENT CHANGE IN RATE
Forgery/counterfeiting	43,833	72,643	91,991	77,692	+39%
	28.9	34.9	46.8	40.3	
Fraud	76,861	261,787	320,046	211,177	+116%
	50.7	125.7	162.9	109.7	
Embezzlement	8,172	7,885	11,605	13,836	+33%
	5.4	3.8	5.9	7.2	

SOURCE: Data compiled from Federal Bureau of Investigation, *Crime in the United States* (Washington, DC: U.S. Government Printing Office, published annually).

motor vehicle theft. The Uniform Crime Reports, however, include forgery/counterfeiting, fraud, and embezzlement in their tallies of arrests (which represent only offenders who are caught). As Table 5.2 indicates, arrest rates for all these offenses have risen dramatically since 1970, even if we control for population growth (rate per 100,000 population). Both the number and the rate of arrests for fraud are higher than those for embezzlement and forgery, although arrest rates for the latter crimes have increased as well.

Increases in white-collar crime reflect employment trends. The proportion of the U.S. population employed in jobs that provide access to information and financial accounts is increasing, and as a result more people have access to criminal opportunities involving misuse of authority and funds.²⁶ As Americans move further away from agriculture and manufacturing to jobs in service industries, high technology, and related professions, access to cash and account numbers by more employees will increase the opportunities for fraud.

Increases in white-collar crime also will reflect demographic trends. The average age of the U.S. population is rising. In 1970 the median age was 27, in 2000 it was 35, and by 2025 it will be about 40.²⁷ The aging of the U.S. population is due to a low birthrate combined with the fact that people are living longer than earlier generations did. The net result is more people in the “white-collar crime-prone” over-twenty-five age group. The majority of those arrested for forgery, embezzlement, and fraud are over twenty-five.

**INCREASES IN
WHITE-COLLAR
CRIME**

Why Is Computer Crime a Growing Threat?

The United States and much of the rest of the world has become completely dependent on computers and electronic telecommunications. Most U.S. households now have computers, as do the vast majority of governments,

businesses, and schools. In the very near future, computers will become as central to our lives at home as they already are at work for most people. The opportunities for misuse of information systems and communication technologies grow daily.

The spread of the automobile early in the twentieth century nearly doubled the number of offenses named in the criminal codes of the United States, and the dominance of the computer is likely to have the same impact in the twenty-first century. Automobiles provided opportunities for illegal activity ranging from substandard manufacturing and repair frauds to auto theft. Computers will have a similar impact as computer viruses and cybertheft threaten people's property and the public order. Legal codes are being modified to eliminate opportunities for crime or misuse, much as changes were needed when automobiles became commonplace.

COMPUTERS AS INSTRUMENTS OF CRIME

■ computer crime

Crimes in which computers are used as the *instrument* of the offense, and crimes in which computers are the *object* of the offense.

Types of Computer Crimes

Computers are most often used to steal, but they can be used to commit other crimes as well. Different types of **computer crime** can be grouped into two basic categories: crimes in which computers are used as the *instrument* of the offense, and crimes in which computers are the *object* of the offense. Computers are used as an instrument in crimes of theft such as embezzlement, fraud, or larceny by computer. For example, the controller at Halifax Technology Services admitted embezzling \$15 million by generating corporate checks to herself over a period of three years. She was sentenced to six and a half years in prison, and she must make repayment at a rate of no less than \$500 per month until the debt is repaid.²⁸ Computers can also be instruments of crime when they are used for purposes of extortion or harassment. The spread of computer viruses, hidden programs that annoy a user or threaten to alter a user's computer files, is an example. Thousands of Internet users received unsolicited e-mails stating that their orders had been processed and their credit card would be charged \$300, but these people had not ordered anything. They were advised to call a phone number with a 767 area code if they had questions. The phone number turned out to be a phone sex line that incurred an automatic charge when connected. The number was located in the West Indies. The conspirators received their money from the phone companies who charged the customers for their connection to the phone sex line. The FTC obtained a court order to freeze the funds collected by phone companies for calls to the phone sex number.²⁹ This scheme illustrates the fact that criminal behavior in the new millennium will involve more sophisticated ways to steal and that the response of the criminal justice system will have to be more sophisticated as well.

Computers can be the object of a crime when the intention is to cause damage to computer hardware (machines) or software (programs). Data destruction and theft or vandalism of computers or programs are examples of such crimes. Likewise, computers can be the object of crime when the intention is to alter data stored in them. Attempts to alter financial state-

COMPUTERS AS OBJECTS OF CRIME

TABLE 5.3 Types of Computer Crime

COMPUTER AS INSTRUMENT	COMPUTER AS OBJECT
Theft by computer (using a computer as a tool to steal)	Damage to software/hardware (physical or electronic damage to computers or computer programs)
Harassment/extortion (using a computer as a means for intimidation or threats)	Data alteration (changing information for undue advantage or revenge)

SOURCE: *Crime in America: Some Existing and Emerging Issues* by Albanese, Jay. © 1993. Reprinted by permission of Prentice-Hall, Inc., Upper Saddle River, NJ.

ments, credit histories, or college grades are examples of this type of computer crime. In other cases, privileged or confidential information, such as software or company secrets, can be altered for purposes of sabotage or copied and sold for illicit profit. Table 5.3 illustrates the variations within the two general categories of computer crime.

Consequences of Computer Crime

The most common form of computer crime is theft by computer. The computer manager at King Soopers stores in Colorado was charged with stealing \$2 million by manipulating computer records at the stores while he was supposed to be fixing “bugs” in the system.³⁰ Increasingly, computers and high-quality color printers are used to counterfeit U.S. currency. Of the \$40 million in counterfeited money seized annually, about half is computer generated.³¹ In these cases computers are used as an instrument to carry out thefts in the form of embezzlement and fraud.

Growing use of the Internet to make purchases has resulted in frauds where buyers and sellers fail to live up to their computer-based agreement. Bidding on products via e-mail auctions has become an extremely popular form of Internet purchasing, but about 80 to 90 percent of the complaints received by the Federal Trade Commission involve instances where a buyer pays for an item but never receives it from the seller. The FTC reports that complaints about Internet bidding fraud have increased dramatically. The average loss per consumer is estimated at approximately \$300.³²

Examples of computer crimes abound. Kevin Mitnick was charged with four counts of fraud for using a friend’s office computer to break into the computer system at Digital Equipment Corporation. Mitnick copied software that had cost Digital \$1 million to develop. He was also charged with electronically entering the Leeds University computer system in England and transferring his telephone charges to a nonexistent MCI long-distance account. Mitnick pled guilty to charges of penetrating business computer systems and causing millions of dollars in damage.³³ In another case, computer

CYBERTHEFT

**HACKER
HARASSMENT**

hackers apparently stole \$12 million in telephone charges from NASA over two years, using long-distance credit card numbers.³⁴ These are examples of a trend toward using computers as a “burglar’s tool” to conduct theft.

Another type of computer crime is the use of a computer to harass or extort a victim. Perhaps the most notorious case of this type is that of Donald Burleson, who inserted a virus (a program that continuously duplicates itself, interfering with the normal operation of computers) into the computer system at a brokerage firm from which he had been fired. The virus erased 168,000 sales commission records.³⁵ Robert Morris, a twenty-three-year-old graduate student, released a macrovirus that brought more than 6,000 university, research, and military computers to a standstill, although no information was taken or lost. A computer “worm” outbreak in 2002 and 2003 prompted calls for better regulation of the Internet, which has yet to occur.³⁶ Many other viruses have been planted in computer programs. Some are relatively innocuous, flashing “Peace” or other messages on thousands of computer screens; others can be extremely harmful. The potential for damage has intensified efforts to improve security technology.

CYBERTERRORISM

A twenty-one-year-old college student in New Jersey was charged when he sent 24,000 e-mail messages to two administrators, who promptly revoked his computer privileges.³⁷ Nine regional Internet service providers were infiltrated by hackers—individuals with sophisticated knowledge who go to great lengths to infiltrate computer systems.³⁸ In each of these cases the computer was used as an instrument to harass, invade privacy, or extort a victim. Hackers were detected in U.S. military computers more than 2,000 times during the 1990s, usually attempting to steal software or data or to leave viruses.³⁹ Although classified information has not been accessed, the potential threat is clear.

**SOFTWARE
PIRATING**

Another type of computer crime involves damage to hardware or software. The damage can be physical or can exist in terms of competitive value. For example, Microsoft Corporation, working with U.S. marshals, seized more than \$1 million in counterfeit software in Los Angeles that had been produced by ten illicit businesses.⁴⁰ Pirated software has been smuggled to Hong Kong and elsewhere, where copies of programs such as Windows are sold for only 5 dollars.⁴¹ Printed matter and photographic images also are pirated in acts of copyright infringement.

In some computer crimes the object is acquisition or alteration of data for an unlawful purpose. During the 1980s a computer systems manager at Lawrence Berkeley Laboratory in California realized that an unauthorized user was looking at his computer files, so he set up a phony “Star Wars” computer file that the hacker could not resist. The suspect was eventually tracked to Hanover, West Germany, where three people were charged with selling secrets to the Soviet Union.⁴² In the late 1980s the FBI’s Computer Intrusion Squad found that 30 percent of large corporations and government agencies it surveyed admitted that their computer systems had been penetrated by outsiders during the previous year; 55 percent reported unauthorized access by insiders.⁴³

Rates of computer crimes of all types are increasing, posing problems for law enforcement. A survey of 250 businesses found that the dollar value of losses from computer crimes totaled \$137 million. Thefts of proprietary company information rose to approximately \$1.7 million.⁴⁴ An FBI and Computer Security Institute survey of 163 businesses reported combined annual losses of \$124 million.⁴⁵ Employees account for nearly two-thirds of suspected cases of computer crime, and some estimates place the number as high as 90 percent. In addition, many huge losses likely go unreported because companies wish to avoid bad publicity and embarrassment, especially if the value of their stock is likely to decrease as a result.

The impact of cybertheft on consumers is evident. In one year two members of a computer hacking group stole 1,749 credit card numbers.⁴⁶ This type of activity has resulted in growing numbers of instances of **identity fraud**, in which false identification and credit cards are manufactured based on personal information stolen without the victim's knowledge. The criminal then uses the fake cards to spend lavishly, ruining in the process the victim's financial standing and credit rating. Although credit card insurance often covers much of the financial loss, victims of identity fraud must reestablish their credit ratings and personal reputation, a process that can take several years. The U.S. Secret Service reports that actual identity fraud losses are \$745 million per year.⁴⁷

The causes of computer crime have not been studied extensively, but a survey of 600 university students found that 34 percent had pirated software and 16 percent had gained illegal access to a computer system. The study found that in many cases these behaviors were learned from others or imitated.⁴⁸ A complication in understanding the nature and scope of computer crime is the fact that businesses seldom want to admit to vulnerability and therefore tend to underreport breaches of computer security. In 1996 the Department of Justice established its Computer Crime and Intellectual Property Section to investigate and prosecute computer-related crimes. Thus far, the biggest challenge has been convincing businesses to report these offenses.⁴⁹

Despite these problems, there have been some notable successes in efforts to combat computer crime. Many of these cases have resulted from work of the FBI's National Computer Crime Squad, which commenced operations in 1992. Undercover sting operations and the sharing of businesses' information about suspected computer hacking are the two most common methods of investigation. In 1996, for example, seventy-eight people were convicted for trading child pornography over the Internet in an FBI sting operation.⁵⁰ A thirty-seven-year-old computer repairman was found to have infiltrated Internet service providers and collected 100,000 credit card numbers. He was ready to sell a CD-ROM with these stolen numbers on it for \$260,000 at San Francisco Airport but walked into an FBI sting operation.⁵¹ Two raids on suspected Internet gambling operations in the Northeast found proceeds estimated at \$56 million. In sum, it appears that computers are being used to commit both white-collar and organized crimes and that improved law enforcement sophistication is needed to combat them.

IDENTITY FRAUD

■ identity fraud

Manufacture and use of false identification and credit cards based on personal information stolen without the victim's knowledge.

CAUSES OF COMPUTER CRIME

THE NATIONAL COMPUTER CRIME SQUAD

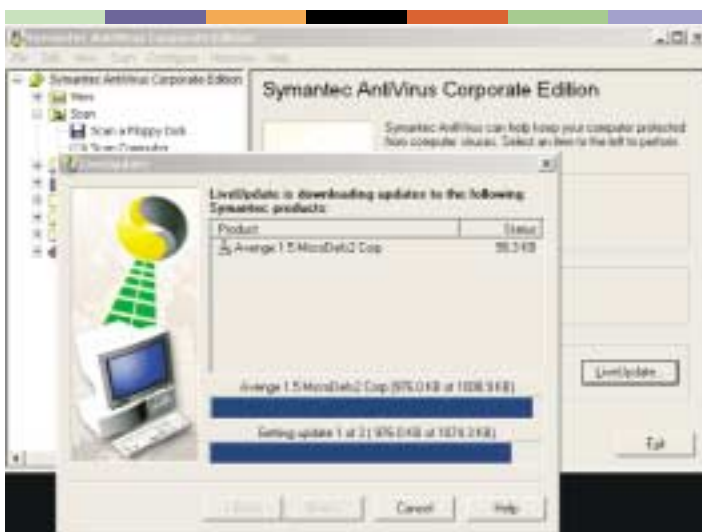
How Does Organized Crime Operate?

■ organized crime

A continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through the use of force, threats, monopoly control, and/or the corruption of public officials.

ORGANIZED VERSUS WHITE-COLLAR CRIME?

In the crime suggested by this photograph, is the computer the object or the instrument of the crime? What is the difference? How is computer crime becoming a threat to individuals, businesses, national infrastructures, and global security? What impact do you think computer crime will have on criminal law and the American criminal justice system?



Organized crime has always fascinated people as a form of criminal behavior, yet its definition and true scope often are unclear. The President's Commission on Law Enforcement in the mid-1960s concluded that "our knowledge of the structure which makes 'organized crime' organized is somewhat comparable to the knowledge of Standard Oil which could be gleaned from interviews with gasoline station attendants."⁵² A similar commission appointed by Ronald Reagan, reporting in 1987, also did not offer any clear definition of organized crime. One definition of **organized crime**, based on the work of researchers in the field, reads as follows:

*Organized crime is a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through the use of force, threats, monopoly control, and/or the corruption of public officials.*⁵³

Even this definition is incomplete, however. For example, how does an otherwise legitimate corporation that collects toxic waste but dumps some of it illegally fit into this definition? Is a motorcycle gang that sells drugs as a sideline part of organized crime? What about a licensed massage parlor that offers some customers sex for money? The National Advisory Committee on Criminal Justice Standards and Goals has recognized that there are more similarities than differences between organized crime and so-called white-collar crime: "The perpetrators of organized crime may include corrupt business executives, members of the professions, public officials, or members of any other occupational group, in addition to the conventional racketeer element."⁵⁴

At the same time, important differences exist between organized and white-collar crime. Perhaps the most significant distinction is the fact that white-collar crimes generally occur as a deviation from legitimate business activity. Organized crime, on the other hand, takes place through a continuing criminal enterprise that exists to *profit primarily from crime*.

It is important to keep in mind the fact that organized crime is not restricted to the activities of criminal syndicates. As Henry Pontell and Kitty Calavita concluded in their study of the savings and loan scandal of the 1980s, if we apply the term *organized crime* to continuing conspiracies that include the corruption of government officials, "then much of the savings and loan scandal involved organized crime."⁵⁵ In interviews with the Federal Bureau of Investigation, the Secret Service, and regulatory agencies, Pontell and Calavita found a "recurring theme" of conspira-

cies between savings and loan officials (“insiders”) and accountants, lawyers, and real estate developers (“outsiders”) that operated as a continuing criminal enterprise. If we compare these kinds of corrupt relationships with more traditional organized crime techniques such as no-show jobs at construction sites or payoffs for “protection,” we find that they are more similar than different. Examples such as this illustrate that much of the crime committed by private corporations, politicians, and government agencies is as serious and harmful as the organized crimes of criminal enterprises.⁵⁶

A Typology of Organized Crime

What types of illegal acts are we referring to when we speak of organized crime? Organized crime falls into three basic categories: provision of illicit services, provision of illicit goods, and infiltration of legitimate business. Within each of these categories are specific crimes that often come to the attention of the criminal justice system.

Provision of illicit services involves attempts to satisfy the public’s demand for certain services that may not be offered by legitimate society. Specific crimes in this category include loan-sharking, prostitution, and certain forms of gambling. Loan-sharking is the lending of money at an interest rate above that permitted by law. Organized prostitution offers sex for pay on a systematic basis. Numbers gambling is a type of lottery that operates without the approval of the state.

Provision of illicit goods involves offering particular products that a segment of the public desires but cannot obtain through legitimate channels. The sale and distribution of drugs and the fencing and distribution of stolen property are examples of crimes in this category. There is a great demand for drugs, such as marijuana, cocaine, valium, and heroin, that are either illegal or distributed under very strict regulations imposed by government. In a similar way, many people desire to buy products at the lowest possible price, regardless of how the seller originally obtained them. In response to this demand, organized criminals fence stolen merchandise, buying stolen property and then selling it to customers who do not care where it came from.

The third category of organized crime is infiltration of legitimate business. This is often characterized by **racketeering**, which involves an ongoing criminal enterprise that is maintained through a pattern of criminal activity. Labor racketeering and the takeover of waste disposal companies are examples of this type of crime. Labor racketeering involves the use of force or threats to employers or employees that if money is not paid, violence, strikes, and/or vandalism will result. In a similar way, organized crime syndicates have taken over waste disposal companies by coercing the legitimate owners to sell the business or have it operated by an outsider. Having the use of a legitimate business allows an organized crime figure to engage in **money laundering**. This is a method of “washing” illegally obtained money (e.g., money from drug sales or gambling proceeds) by making it appear that the money was earned legally as part of the legitimate business.

PROVISION OF ILLICIT SERVICES

PROVISION OF ILLICIT GOODS

INFILTRATION OF LEGITIMATE BUSINESS

■ racketeering

An ongoing criminal enterprise that is maintained through a pattern of criminal activity.

■ money laundering

A method of “washing” illegally obtained money (e.g., from drugs or gambling proceeds) by making it appear as if the money were earned legally as part of a legitimate business.

TABLE 5.4 A Typology of Organized Crime

TYPE OF ACTIVITY	NATURE OF ACTIVITY	HARM
Provision of illicit goods and services	Gambling, loan-sharking, prostitution, distributing narcotics and stolen property	<ul style="list-style-type: none"> • Consensual activities • No inherent violence • Economic harm
Infiltration of legitimate business	Coercive use of legal businesses for purposes of exploitation	<ul style="list-style-type: none"> • Nonconsensual activities • Threats, violence, extortion • Economic harm

SOURCE: Albanese, *Organized Crime in Our Times* (Lexis/Nexis/Anderson, 2004).

Table 5.4 illustrates this typology of organized crime. Provision of illicit goods and services is distinguished from infiltration of legitimate business by its consensual nature and by the lack of direct or inherent violence. That is, organized crime figures who offer illegal betting, loan-sharking, or drugs rely on the public's unsatisfied demand for these services. They also rely heavily on return business, so they want the illicit transaction to go well. It is very unusual for criminal syndicates to *solicit* business. Instead, those interested in illicit goods and services seek out the providers. But although violence plays no inherent role in the activities themselves, bad debts cannot be collected through the courts, as they can for loans and sales in the legitimate market. Therefore, violence or threats occur when one party to the transaction feels cheated or shortchanged and has no legal alternative for resolving the dispute. Violence also can occur when an organization attempts to control or monopolize an illicit market. If a group wishes to corner the market on illicit gambling in a particular area, for example, it may threaten or intimidate its illicit competitors. These threats are an enforcement mechanism rather than a part of the activity of providing illicit goods and services.

The infiltration of legitimate business is more predatory than the provision of illicit goods and services. In this case organized crime groups attempt to *create* demand for their services rather than exploiting an existing market. Demands for "protection" money or demands that employers provide no-show jobs in return for avoidance of property damage, work stoppages, or violence illustrate the predatory nature of this type of crime. In legal terms, organized crime uses coercion or extortion in the infiltration of legitimate business. "Protection" of prostitutes from robbery and assault in return for coerced payments to pimps is another example of the predatory nature of organized crime.

Organized Crime Offenders

CRIME "FAMILIES"

Ethnicity is a common basis for categorizing organized crime, but this is misleading. A growing body of evidence shows that organized crime is not limited to the activities of a single, or even a few, ethnic groups. The Pres-

ident's Commission on Organized Crime in the 1980s described "organized crime today" as being carried out by eleven different groups:

- La Cosa Nostra (Italian)
- Outlaw motorcycle gangs
- Prison gangs
- Triads and Tongs (Chinese)
- Vietnamese gangs
- Yakuza (Japanese)
- Marielitos (Cuban)
- Colombian cocaine rings (drug cartels)
- Irish organized crime
- Soviet organized crime (the "Russian Mafia")
- Canadian organized crime.⁵⁷

This curious mixture includes groups defined by their ethnic or national origin, by the nature of their activity (cocaine rings), by their geographic location (prison gangs), and by their means of transportation (motorcycle gangs). While such attributes may help describe a group, they are not very useful as explanations of behavior. Moreover, there is evidence that these and other organized crime groups sometimes work together.⁵⁸

Ethnicity, therefore, is not a very powerful explanation for the existence or the causes of organized crime. This conclusion is supported by several studies of ethnically based organized crime. These studies show not only that no single ethnic group or combination of groups accounts for most organized crime, but also that as an explanation for organized crime, ethnicity is secondary to local opportunities for crime. A study by historian Alan Block of the illicit cocaine trade in New York City in the early twentieth century identified Jews as major players but also found evidence of considerable interethnic cooperation among New York's criminals. There was evidence of involvement by Italians, Greeks, Irish, and blacks, who did not always work within their own ethnic groups. Block described these criminals as "entrepreneurs" who were not part of one particular organization but were involved in a "web of small but efficient organizations."⁵⁹

A study by Patricia Adler of the underground drug market in one community found that the market was largely competitive. Participants "entered the market, transacted their deals, [and] shifted from one type of activity to another" in response to the demands of the market rather than the dictates of any ethnically based organization.⁶⁰

Similarly, in a study of illegal gambling and loan-sharking in New York, Peter Reuter found that economic considerations dictated entry into and exit from the illicit marketplace. Reuter concluded that these criminal enterprises were "not monopolies in the classic sense or subject to control by some external organization."⁶¹ Instead, local market forces shaped criminal behavior—more so than ethnic ties or other characteristics of the criminal groups.

In a classic ethnographic study, Francis Ianni became a participant-observer of an organized crime group for two years; he also made observations

ETHNICITY AND ORGANIZED CRIME

CRIME SYNDICATES

■ crime syndicate

A system of loosely structured relationships among groups and individuals involved in organized crime.

of two other criminal groups. He found these groups to “have no structure apart from their functioning; nor do they have structure independent of their current ‘personnel.’”⁶² Joseph Albini’s pioneering study of criminal groups in the United States and Italy reached a similar conclusion. Rather than belonging to an organization, those involved in organized crime formed relationships based on the particular activity they were engaged in at any given time. A **crime syndicate**, Albini concluded, is “a system of loosely structured relationships functioning primarily because each participant is interested in furthering his own welfare.”⁶³ These studies suggest that the structure of organized crime groups is derived from the activities they are engaged in, rather than from preexisting ethnic ties.

National and International Aspects of Organized Crime

The true extent of organized crime is unknown. Characteristic organized crimes such as conspiracy, racketeering, and extortion are not counted in any systematic way. Other offenses are known only when they result in arrests. The problems with relying on arrests as a measure of criminal activity are apparent: Much crime is undetected, some that is detected is not reported to police, and arrest rates go up or down depending on police activity and do not necessarily reflect levels of criminal activity. However, arrest data are the only available statistics, and they provide some indication of the amount of organized crime committed each year.

The Federal Bureau of Investigation tabulates arrests for several offenses that are characteristic of organized crime. Trends in these arrests from 1970 to 2001 are presented in Table 5.5. As can be seen, arrests for three of the four categories of offenses increased markedly over the thirty years shown, whereas arrests for gambling dropped dramatically. These increases and decreases can be attributed to two primary factors: changes in law enforcement priorities and changes in the overall population and in the numbers of police. Both the U.S. population and the number of sworn police officers in the United States have grown significantly since 1970. Therefore, one would ex-

ARRESTS FOR ORGANIZED CRIME

TABLE 5.5 Arrests for Crimes Related to Organized Crime

OFFENSE	1970	1980	1990	2001	30-YEAR CHANGE
Drug abuse violations	265,734	351,955	785,536	1,091,240	4 times higher
Gambling	75,325	37,805	13,357	7,769	9 times lower
Prostitution and commercialized vice	45,803	67,920	80,888	58,638	25% higher
Stolen property (buy, receive, possess)	46,427	76,429	119,102	84,047	2 times higher

SOURCE: Data compiled from the Federal Bureau of Investigation, *Uniform Crime Report* (Washington, DC: U.S. Government Printing Office, published annually).

pect a “natural” increase in numbers of arrests, simply because there are more potential offenders and victims in the population, as well as more police looking for them.

At the same time, the public mood has shifted, especially with regard to gambling and drugs. Gambling in many forms has been legalized in a majority of the states in response to a shift from the perception of gambling as a vice to its perception as a form of recreation.⁶⁴ Conversely, public concern about drugs increased over the same period. The large increases in drug arrests (four times higher in 2001 than in 1970) are matched only by the huge decline in gambling arrests (nine times lower over the same period). These changes clearly indicate shifting public—and hence law enforcement—views regarding the seriousness of these forms of criminal behavior.

It is possible that the rates of these offenses have also changed over the years, but we cannot determine this from arrest statistics. The fact that prostitution and commercialized vice arrests increased over thirty years, and that arrests for stolen property nearly doubled from the 1970 level suggests that more police, greater enforcement efforts, and increases in the numbers of cases combined to produce these large increases in arrests.

In the future, organized crime is likely to pose even greater problems than it has in the past. Technological change and economic globalization are likely to contribute to growth in organized crime. Organized crime groups increasingly are making use of stolen and forged credit cards, airline tickets, cell phones, and currency.⁶⁵ New Visa check cards and MasterMoney cards require only a signature and no personal identification number to withdraw funds, making it easy for forgers to withdraw large amounts of money quickly.⁶⁶ With each advance in technology, new criminal opportunities emerge. Gambling and pornography on the Internet and banking by telephone and by personal computer are examples of new opportunities for both organized crime and white-collar crime to grow in the future.

Just as advances in technology and the fall of Communism have made worldwide communication and travel much easier in recent years, they have also made the commission of crime much easier. Passenger miles flown on international commercial flights have increased by twenty times since 1970, to more than 600 billion miles per year. Global imports have increased by a factor of ten to \$3,500 billion over the same period.⁶⁷ International smuggling, drug distribution, alien smuggling, hijacking, and political crimes have grown in proportion to the growth of international communication and movement among countries. As criminal justice researcher Jonathan Winer has observed, “The very networks that legitimate businesses use to move goods so cheaply are the same networks that criminals use to move illicit goods just as easily.”⁶⁸

International Stolen Vehicle Trade One manifestation of **transnational crime** is the growing international trade in stolen vehicles. Of the 1.5 million vehicles stolen each year in the United States, approximately 200,000 are shipped overseas for resale. As recently as the mid-1980s, that international market barely existed.⁶⁹ To hide stolen cars from investigators,

TRENDS IN ORGANIZED CRIME

■ **transnational crime**
Organized crime that takes place across two or more countries.

TABLE 5.6 Stolen Vehicle Recoveries in Foreign Countries

COUNTRY	NUMBER OF STOLEN VEHICLES TRACED TO THE COUNTRY IN 1998	NUMBER OF STOLEN VEHICLES RECOVERED, 1996–1998
Mexico ^a	6,345	6,011
Belize	N/A	0
Guatemala ^a	64	10
Dominican Republic ^a	37	33
Costa Rica	N/A	2
Panama	N/A	10
Venezuela ^a	55	15
El Salvador	N/A	0
Honduras ^a	36	0
Nicaragua	N/A	9
Poland ^a	19	27
Russia	N/A	0

^aThese countries, along with Germany (twenty-three vehicles), Ecuador (twenty-one vehicles), Haiti (twenty-one vehicles), and Belgium (sixteen vehicles), comprise the top ten countries in which stolen vehicles were located in 1998.

SOURCE: U.S. Comptroller General, *Efforts to Curtail the Exportation of Stolen Vehicles* (Washington, DC: U.S. General Accounting Office, 1999).

thieves often conceal them behind false container walls or in large steel containers bound for overseas shipping. A single ship holds as many as 4,000 steel containers, each as large as a semi-trailer. Ten million containers leave the Los Angeles–Long Beach seaport alone each year, and the United States has 130 seaports. Criminals pay thieves to steal desired cars off the street; or criminals buy or rent the cars by using false identification and making a cash deposit, then drive away never to return. On the foreign end, buying and registering stolen vehicles is not very difficult. Some countries have no central registry of vehicles. In others, aspiring car owners can bypass registration requirements with cash payoffs. In some countries crimes of violence and political unrest are the focus of police attention, so police are not overly concerned with imports of stolen cars.

The U.S. Customs Service reports that nearly one million vehicles are presented for export from the United States annually. Customs identifies and seizes nearly 7,000 of these as stolen vehicles with a total value of over \$100 million. The National Insurance Crime Bureau estimates that 200,000

stolen vehicles are exported each year, so clearly the vast majority of illegal exports are undetected.⁷⁰ Table 5.6 illustrates that most stolen vehicles are transported to Central America, South America, and Eastern Europe.

Major reasons why people in many countries do not simply buy the cars legitimately are lack of availability and huge import duties. A \$50,000 Lexus, for example, was found selling in a Thailand showroom for \$180,000.⁷¹ The total cost of international vehicle smuggling is estimated at \$1 to \$4 billion annually. As a representative of the National Insurance Crime Bureau remarked, “It’s getting to be of epidemic proportion.”⁷² In response to this situation Interpol has established a database on reported stolen vehicles suspected of being transported abroad. More than thirty countries have been participating, and more than one million vehicles are in the database, which has been used to track the origin of seized vehicles in countries around the world.⁷³

Drug Smuggling The problem of international automobile smuggling is mirrored in international drug smuggling. Drug smuggling begins at a source country where coca or opium is grown, usually in Central or South America or Asia. Next, the raw plant must be processed. This can be done in the source country or in a nation where smuggling is relatively easy. Once the substance has been transformed into a consumable product, it must be smuggled to the consumer drug market; North America and Europe are the largest markets. After the drug has been sold to the consumer, money must be laundered through a legitimate business and transferred overseas; or else

U.S. CUSTOMS

large amounts of cash must be physically smuggled by couriers back to the manufacturing and source countries. As discussed earlier, the laundering consists of reporting the drug money as part of the income from a legitimate business, such as a restaurant or other business that has a large number of cash transactions, making the money look as if it were lawfully earned as part of the legitimate business.

Here is an example of how the international drug trade works in practice. Nigerian heroin smugglers recruited non-Nigerian residents of Dallas to serve as couriers, smuggling heroin into the United States. The recruiters provided airline tickets and expense money for the couriers, in addition to a salary of \$5,000 to \$10,000 per trip. For each batch the first courier was sent to Thailand, the heroin source, and took the heroin from there to an intermediate nonsource nation (such as the Philippines, Kenya, Poland, or western Europe), where it was delivered to a second courier. The second courier concealed the heroin in a suitcase or strapped it to his or her body, and smuggled it into the United States. The strategy was designed to deceive U.S. authorities, who would not suspect a courier who had not come from the source country.⁷⁴ This scheme capitalizes on multiethnic cooperation among criminals—and points to the need for international cooperation and surveillance by law enforcement agencies.

The two primary opportunities for preventing drug smuggling occur at the courier stages, when the finished product is being smuggled to the market or when the illicit cash is being returned from the consuming country. In the United States, profiles have been established for drug couriers and for “high-risk” and “source” nations and airports that lack effective controls on drug manufacturing or contraband. The profiles are descriptions of travelers who appear likely to be carrying drugs or cash, such as persons who are making short international trips, carry little luggage, appear in a hurry, and pay for their tickets in cash.⁷⁵

Illegal Immigration Illegal immigration is a third example of transnational crime. There are many people throughout the world who wish to come to the United States and other developed countries but have little chance of lawful immigration. Chinese smuggling rings have transported illegal immigrants to New York City by boat for a charge of \$30,000 or more per person. Sometimes the “cargo” is smuggled by boat to Canada or Mexico and then transported by land to the United States.⁷⁶ Sometimes smugglers ship this human cargo in containers, causing injury and death.⁷⁷ The huge smuggling fee often turns the new arrivals into virtual slaves to their transporters. Because they are illegal aliens, it is difficult for these immigrants to obtain legitimate employment, so they often are exploited in



In what ways can organized crime often involve international, or transnational, crime? According to statistics on international crime, what three kinds of contraband are most likely to be found on a vessel such as the one shown in the photo?

HOW THE DRUG TRADE WORKS

TARGETING COURIERS

**TRAFFICKING
IN PERSONS**

sweatshops by unscrupulous employers, become prostitutes or drug couriers, or become involved in criminal activity to raise the money to pay their smuggling fee.⁷⁸ The impacts are felt by the U.S. criminal justice system as well as by the illegal immigrants themselves. Nearly half of the non-U.S. citizens prosecuted in federal court are living in the United States illegally. Most have been charged with drug or immigration offenses, which have risen by more than 10 percent per year over the last decade. Nearly 20,000 noncitizens are now incarcerated in federal prisons.⁷⁹

There is also concern about illegal immigrants from terrorist countries who enter Canada and then slip into the United States. Ahmed Ressam, an Algerian immigrant to Montreal, is awaiting trial in the United States on charges he tried to smuggle explosives into the United States. Canada's immigration laws are more lax than those in the United States, and Canadian police agencies are aware of 350 suspects in Canada who are linked to 50 different radical groups. Canada is debating stronger immigration and surveillance measures to prevent it from becoming a "Club Med for terrorists" who might target Canada or the United States.⁸⁰

Immigrants continue to be victimized by their smugglers in what is called trafficking in persons. Many are brought to the United States using false promises, fraudulent contracts, or outright coercion. Once they arrive, they are forced to work as slaves for their captors, often in forced labor and prostitution. The largest case to date involved Kil Soo Lee who headed a group that trafficked 200 Vietnamese and Chinese women to American Samoa as sewing machine operators in a garment factory. They were forced to work there for up to two years under extreme food deprivation, beatings, and physical restraint. The victims were held in a barracks and guarded at all times to prevent their escape. Virtually all the money they made went to their captors.⁸¹ As William McDonald has remarked, "The problems of organized crime involved in the fraud, corruption, smuggling, and victimization associated with illegal immigration represent a growing area of need for transnational police cooperation which threatens to eclipse international drug trafficking as a social problem in the global village."⁸²

U.S. authorities are able to identify only a small percentage of the vessels carrying illegal immigrants. Given the vast extent of the nation's borders and the inability of any nation to search every person, car, boat, and plane that crosses its borders, there is a clear need for international cooperation and coordination of law enforcement efforts.

What Are the Impacts of Terrorism and Hate Crimes?

Terrorism and hate crimes are criminal acts committed for political or social purposes. They are distinguished from most other forms of crime in that these offenders usually have no personal financial motive. Instead, they attempt to make a "point" that goes beyond their own self-interest. Their pur-

pose may be the overthrow of the government, or they may wish to publicize an unpopular opinion. Hate crimes always involve prejudice in some form—usually racial or ethnic in nature. Terrorism sometimes entails prejudice, but more often it stems from political motives or causes. The FBI defines **terrorism** as

*the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.*⁸³

Hate crimes can also be defined in this way. The primary difference is the target: In the case of terrorism, the government is usually the target; in the case of hate crimes, a particular minority group is usually the target. Hate arises from prejudice against people's race, ethnicity, religious affiliation, or sexual orientation. In a particularly gruesome case, Aaron McKinney was convicted for the torture killing of gay college student Matthew Shepard in Wyoming.⁸⁴

Both terrorism and hate crimes are new and growing concerns for the U.S. criminal justice system. Before the 1980s major acts of terrorism occurred almost exclusively in foreign countries, and hate crimes had not been defined as such and were not counted in any systematic way. This changed in 1993 with the bombing of the World Trade Center in New York City, which killed six people. The offenders were convicted and the mastermind was sentenced to 240 years in solitary confinement.⁸⁵ Subsequent terrorist events in the United States included the 1995 Oklahoma City bombing, which killed 168 people, followed by the September 11, 2001, attacks on the World Trade Center and Pentagon, killing 3,047 people. Acts of terrorism and hate crimes now occur regularly in the United States as well as in other parts of the world. Aircraft bombings, plots against government agents, church burnings, periodic random killings of minorities, and actions by hate groups founded on a premise of racial inequality illustrate the extent of the problem in the United States.⁸⁶

■ terrorism

Offenses designed to intimidate or coerce a government or civilians in furtherance of political or social objectives.

■ hate crimes

Offenses motivated by prejudice, usually against a particular race, religion, or sexual orientation.

Terrorism and Hate Crime Trends

The number of terrorist incidents in the United States has declined since the 1980s, but the crimes committed are becoming more deadly. Fears of Y2K-related sabotage resulted in heightened security around the world, and surveillance efforts resulted in several arrests of persons suspected of terrorist plots.⁸⁷ Law enforcement authorities are giving higher priority to terrorism investigations, with emphasis on the *prevention* of terrorist acts. Trends in the prevention of terrorism in the United States are illustrated in *That's a Fact*. A significant number of terrorist acts have been prevented or interrupted in recent years, and these preventions are increasing (Figure 5A). This trend points to the importance of improved intelligence gathering on terrorist activities, which can anticipate and interrupt planned terrorist activity before it results in damage or death.

Statistics for hate crimes were not collected before the 1990s. In 1991 there were 4,755 reported incidents of hate crimes in the United States. By 2001

THAT'S A FACT

PERSPECTIVES ON TERRORISM

Terrorism was becoming more dangerous even prior to the attacks of September 11, 2001. The National Commission on Terrorism reported in 2000 that injuries and deaths resulting from terrorist incidents were increasing, while the total number of incidents had declined somewhat since 1980. This is displayed in Figure 5A.

How can casualties increase in terrorist incidents, when incidents decline? Why do you believe agencies were slow to coordinate their preparedness for major terrorism incidents prior to September 11, 2001, despite the warnings of the National Commission on Terrorism a year earlier?

Better safeguards in granting visas is an important method to ensure that those connected with terrorists are kept out of the United States. A visa is an official authorization attached to a passport that permits entry and travel within a country. The United States grants thousands of visas each year through the State Department to tourists, workers, students, and other foreign visitors. The U.S. General Accounting Office (GAO), the investigative arm of Congress, has been asked to examine the visa approval process several times in recent years. Their findings reveal important information and communication gaps among U.S. agencies.

The GAO found that the U.S. Departments of State, Homeland Security, and Justice could more effectively manage the visa process if they had clear and comprehensive policies and procedures, and also increased coordination and information sharing among agencies. In a October 2002 report, GAO found that:

- The State Department did not provide clear policies on how consular officers should balance national security concerns with the desire to facilitate legitimate travel when issuing visas; and
- The State and Justice Departments disagreed on the evidence needed to deny a visa on terrorism grounds.

In a June 2003 report, GAO found that the State Department had revoked visas for terrorism concerns, but that:

- The revocation process was not being used aggressively to alert Homeland Security and law enforcement agencies that individu-

als who entered the country before their visas were revoked might be security risks; and

- The process broke down when information on revocations was not being shared between the State Department and appropriate immigration and law enforcement officials.

For example, a detailed analysis of 240 visa revocations found that U.S. Immigration officials did not receive any notice of the revocation from the State Department, and in another forty-seven cases the revocation notice was sent to Immigration twelve days later. The State Department failed to enter sixty-four of these revocations into its own watch list. An analysis of arrival and departure data found that twenty-nine individuals entered the United States *before* their visas were revoked and they may still remain in the

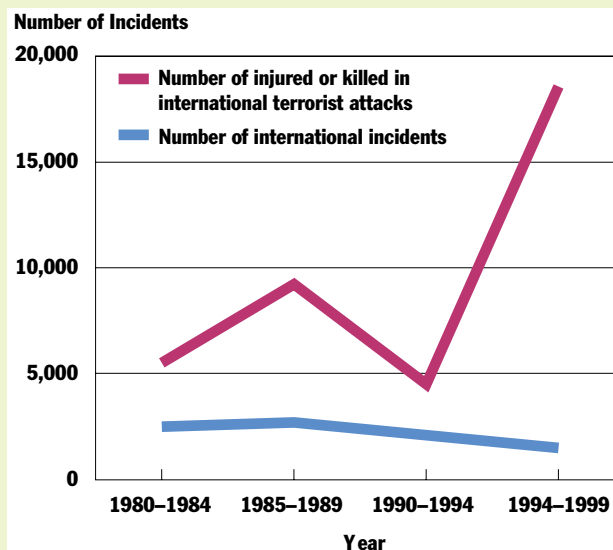


Figure 5A

Terrorism Becoming More Dangerous

SOURCE: National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Washington, DC: U.S. Government Printing Office, 2000).

HATE CRIME STATISTICS

the number had risen to 9,730, an increase of 105 percent. More than 66 percent of these incidents are racial or ethnic in nature, and two-thirds of these involve antiblack motives. Nearly 19 percent of all reported incidents are religious in nature; 57 percent of these are anti-Semitic (anti-Jewish). More than 14 percent of all incidents involve sexual orientation; of these, two-thirds target homosexual males.⁸⁸ It is clear that minority groups are most likely to be the targets of hate crimes, and that prejudice against a particular race, religion, or sexual orientation motivates these offenders.

United States. The GAO concluded, "These weaknesses diminish the effectiveness of the visa process in keeping potential terrorists out of the United States."

The GAO made numerous recommendations to strengthen the visa process as an antiterrorism tool. These focused on specific policies and procedures for the interagency visa revocation process to ensure that when the State Department revokes a visa because of terrorism concerns, the appropriate units within the Departments of State and Homeland Security and the FBI are notified immediately and that proper actions are taken. A diagram of problems in the information flow in visa screening is shown in Figure 5B.

Changes have been made in the visa process since these reports, including a doubling of the number of names and information in the "lookout" system for visa screening. The State Department has said it

is using the GAO recommendations as a road map for making improvements in the visa process.

Why do you believe it is so difficult for large federal agencies to coordinate their efforts in the visa process? If you were in charge, explain how you might balance the need for international workers and visitors against the need to protect against terrorism?

SOURCE: U.S. Comptroller General, *Border Security: New Policies and Increased Interagency Coordination Needed to Improve Visa Process* (Washington, DC: U.S. General Accounting Office, 2003); U.S. Comptroller General, *Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process* (Washington, DC: U.S. General Accounting Office, 2003).

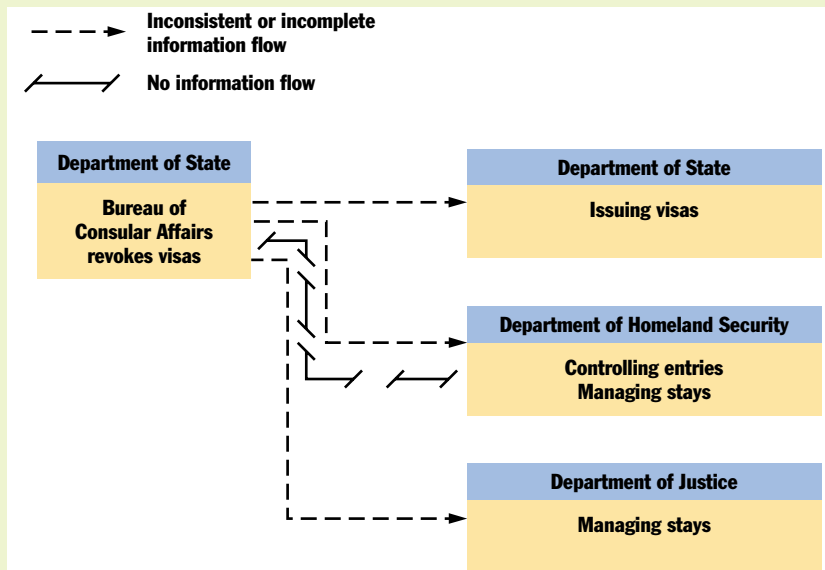


Figure 5B
Gaps in the Visa Revocation Notification System

How Terrorism and Hate Crimes Merge

The following case illustrates how the problems of hate crime and terrorism merge. Two men belonging to an organization known as the Aryan Nations traveled from Idaho to Seattle, Washington, with the intent of exploding a bomb inside a gay bar. They were arrested after transporting the parts required for the bomb, but before they had assembled it. The arrest was based on evidence gathered by an undercover informant who had

ARYAN NATIONS



Sikh children sing "God Bless America" at a community service in California to remember victims of terrorist attacks. Although Sikhs are not Muslims and come from India, they have been targeted in recent hate crimes because the men wear turbans and beards similar to terrorist suspect Osama bin Laden. If terrorism can lead to hate crimes, how would you profile individuals for terrorism investigations?

UNABOMBER

penetrated the Aryan Nations organization and had accompanied the two men on their trip to Seattle. The men were convicted of conspiracy involving interstate travel to kill or hurt human beings in violation of federal law.

The two men appealed their convictions, arguing that there was insufficient evidence of a conspiracy. They claimed that the government had failed to prove beyond a reasonable doubt that there existed an agreement to engage in the crimes charged.⁸⁹ However, the U.S. Court of Appeals found the testimony of the undercover informant, as well as tape-recorded statements of the conspirators, to be convincing evidence of a conspiracy. Before leaving for Seattle, the men had discussed obtaining a bomb from someone else. When that person could not be found, the defendants "actively participated in purchasing the components necessary to build another pipe bomb." Once in Seattle, they sought to borrow a drill from a friend to use in assembling the bomb. According to the testimony of the undercover informant, the two men had discussed the effect an explosion from a pipe bomb would have on a room full of people. In discussing the number of homosexuals that would be killed by such a bomb, they concluded that "the gravel and nails inside it would be lethal." One defendant also told the other that it would be best "to buy pipe and pipe caps for the bombs at various stores."⁹⁰ The court concluded that once a conspiracy has been shown to exist, evidence establishing a defendant's connection with it beyond a reasonable doubt "is sufficient to convict the defendant of knowing participation in the conspiracy," even though the connection may be slight.⁹¹ This case demonstrates that the concerns about criminal organization and conspiracy that arise in hate crimes are nearly identical to concerns posed by terrorism. The planned and conspiratorial nature of the acts, and the political motives behind them, make terrorism and hate crimes serious threats to public safety and to law enforcement.

An infamous case of domestic terrorism is that of Theodore Kaczynski. Called the "Unabomber," Kaczynski pleaded guilty in 1998 to killing three people and injuring two others in five mail bombs. He also admitted to sending an additional eleven bombs that injured twenty-one other people. Kaczynski was a fifty-five-year-old mathematician who believed he was waging a struggle for individual autonomy against the forces of technology. He lived alone in a remote cabin in the woods for twenty-five years. His targets were university professors and others he believed represented the growth of technology. Kaczynski's motives can be viewed both as domestic terrorism and as hate crimes. He had a political agenda, and his choice of victims was based on a strong prejudice against people who advocated technological advancement. Kaczynski ultimately pleaded guilty and was sentenced to life in prison with no chance of parole.⁹²

In place of the radicals of the earlier twentieth century, right-wing extremist groups have attracted supporters in recent years. These groups often adhere to an antigovernment or racist ideology. The FBI has found that recruits to these groups feel displaced by rapid cultural and economic changes and in some cases are "seeking some form of personal affirmation." As U.S.

society continues to change, the FBI predicts that the potential for hate crimes by extremist right-wing groups will increase.⁹³

Prior to September 11, 2001, antiterrorism efforts were splintered among different agencies.⁹⁴ To improve their preparedness to respond to terrorist incidents, federal agencies conducted more than 200 exercises, about a third of which include state and local participants. Agreement on an interagency terrorist response program was slow to develop due to problems in securing appropriate levels of agency participation and in transferring command and control responsibilities in multiagency efforts.⁹⁵ The National Commission on Terrorism, created by Congress after the bombings of U.S. embassies in East Africa, issued a report in 2000 recommending even more aggressive steps to prevent terrorism. These included making the U.S. military the agency to lead the government's response to terrorist attacks, rather than law enforcement agencies. It was also recommended that foreign students in the United States be monitored and that sanctions be taken against nations that fail to cooperate fully with terrorism investigations.⁹⁶ These recommendations sparked some controversy, but they point to flaws in the readiness of the United States in preventing or responding to acts of terrorism.

These warnings and preparations were not sufficient to prevent the attacks of September 11, 2001, which resulted in a new level of fear and concern in the United States about terrorism, and also new legislation designed to accomplish the objectives of the earlier efforts which had fallen short. The USA Patriot Act was passed weeks after the September 11 attacks, and it provides a series of provisions to enhance the government's ability to gather information that may be related to terrorism, including expanded authority to monitor communications among citizens.⁹⁷ The Patriot Act most directly affects police powers, and it is examined further in Chapter 9.

critical thinking exercises

Is the Internet an Avenue for Terrorists?

A twenty-year-old former computer science student pleaded guilty in Boston in 2000 for a hacking spree against targets that included the military and NASA.^a An "urgent" e-mail purportedly from a government agency claimed that bananas from Costa Rica carry a "flesh-eating" bacteria that can eat "2 to 3 centimeters of flesh an hour" resulting in amputation or death. This claim was denied by the U.S. Centers for Disease Control, but a panic was feared. The banana industry called this "just another case of Internet terrorism like the recent hacker attacks on popular web sites."^b These are examples of a growing number of incidents where both government and business Inter-

net sites have been vandalized and sometimes offensive or subversive material posted.

The Internet has come under increasing fire for posting information that is inaccurate, inflammatory, and/or dangerous. A "police brutality" webpage admits to not verifying the facts posted. The publisher of the webpage said, "I don't think twice about badmouthing presidents, newspaper reporters, or other public officials."^c In 1997 the Supreme Court struck down a law barring the posting of "indecent" material on the Internet because that term was too vague. Nevertheless, the government retains the right to prosecute individuals who post obscene material or child pornography on the Internet; these materials are more clearly defined in law.^d

At the same time, the FBI has stated that some Internet sources "are repositories for inflammatory rhetoric which can influence extremists. Databases on the Internet contain recipes for

bombs, dispense information on unconventional weapons, or offer computer viruses for download.^e There are chat rooms for those who hold extremist, racist, sexist, and separatist views. Sometimes these people gather in person to engage in deviant activities. Occasionally these activities are unlawful. There is hate speech on the Internet as well as antigovernment postings, sites that advocate rape and violence, and many other sites that can be considered offensive. Those who spend time surfing the Internet can find a wealth of useful information posted there. But some of that information can also be used for destructive or illegal purposes.

CRITICAL THINKING QUESTIONS

1. Distinguishing harmless speech from harmful action is difficult. Should bomb recipes be barred from publication on the Internet? Why or why not?
2. Should inflammatory rhetoric that incites racial, ethnic, or government hatred be prohibited on the Internet? Why or why not?
3. Does a person have a right to post whatever he or she wants on the Internet, or should there be a standard for Internet content?

NOTES

- a. John Bacon, "Former Student Admits Hacking NASA," *USA Today* (June 30, 2000), p. 3.
- b. David Noack, "Banana Rumor Called 'Internet Terrorism,'" *APBnews.com* (February 25, 2000).
- c. Mark Johnson, "Lawsuits Spur New Rules for Internet," *Richmond Times-Dispatch* (September 9, 1997), p. 12.
- d. *Reno, Attorney General of the United States v. American Civil Liberties Union*, 117 S.Ct. 2329 (1997).
- e. Federal Bureau of Investigation, *Terrorism in the United States* (Washington, DC: U.S. Government Printing Office, 1998), p. 14.

Should There Be Limits on Controlling Pollution?

In 2000 two cruise lines each faced fines of \$50,000 to \$100,000 for violating smokestack emissions standards in Alaska.^a Two oil refiners also agreed to settle air pollution violations in a separate case.^b Ford and Honda reached an out-of-court settlement with the government over the sale of hundreds of thousands of vehicles that did not comply with clean air regulations. The settlement included a \$12 million civil penalty and \$150 million worth of free tune-ups and extended warranties.^c Where do these air pollution standards come from? The Clean Air Act became law in 1970, which was followed with even stricter laws on the state and local level aimed at reducing particulate emissions into the air and ozone. Emission control devices on

automobiles have become standard features since then, as have similar devices on smokestacks of all kinds.

In 2000 a challenge to these standards was issued in a decision by the U.S. Court of Appeals which held that the U.S. Environmental Protection Agency (EPA) "has failed to state intelligibly how much is too much" in determining appropriate emission levels.^d The EPA had reduced the permissible level of ozone from 0.09 to 0.08 parts per million arguing that fewer persons would be harmed under the lower level. The question is how low can the standards be reduced and at what cost to industry and consumers? Similar to other laws of this kind, Congress empowers regulatory agencies like the EPA to set precise standards under the law, the details of which are often too politically controversial for Congress to state in the law itself.^e In this case it was argued that the standards established by EPA are too stringent, resulting in overdeterrence, where the price of a product is raised so high by costs of regulation that companies may cease the activity, thereby hurting society.^f The U.S. Supreme Court agreed to hear this case during 2001 to decide whether the EPA must consider the economic costs of air pollution reductions beyond any public health benefits. The Court addressed the concerns raised by the lower court that the EPA lacked "criteria for drawing lines" between acceptable and unacceptable pollution levels.^g

CRITICAL THINKING QUESTIONS

1. Should public health be the overriding concern in determining legal limits of pollution?
2. If businesses that violate these standards are forced to go out of business, how can this be a bad thing?
3. What are some public health and economic cost indicators you might use to assess the benefits and costs of air pollution standards? How would you attempt to balance their importance?

NOTES

- a. "Cruise Ships Cited for Polluting Alaska," *APBnews.com* (August 4, 2000).
- b. "Two Refiners Agree to Settle Air Pollution Violations," *New York Times* (July 26, 2000), p. A19.
- c. "Ford, Honda Reach EPA Deals: Makers Settle Clean Air Cases," *Automotive News* (June 8, 1998), p. 1.
- d. *State of Michigan Department of Environmental Quality v. U.S. Environmental Protection Agency*, 213 F.3d 663 (2000); *Browner v. American Trucking Association*, 120 S. Ct. 2711 (2000).
- e. Michael Barone, "Reining in the Regulators," *U.S. News & World Report* (June 12, 2000), p. 29.
- f. Mark A. Cohen, "Sentencing the Environmental Criminal," in Mary Clifford, ed. *Environmental Crime: Enforcement, Policy, and Social Responsibility* (Gaithersburg, MD: Aspen, 1998).
- g. Linda Greenhouse, "Justices Broaden Their Look at the Clean Air Act," *New York Times* (May 31, 2000), p. 1.

SUMMARY

WHAT IS MEANT BY POLITICAL AND ECONOMIC CRIMES?

- Sophisticated crimes are characterized by planning and organization. Criminal law punishes criminal planning as the crime of conspiracy.
- Conspiracy takes place when two or more persons agree to commit a crime, or to carry out a legal act in an illegal manner.

HOW CAN WHITE-COLLAR CRIMES BE DEFINED?

- White-collar crimes are distinguished by the manner in which they are carried out. Whereas street crimes are characterized by the use of force or stealth, white-collar crimes are characterized by planning and deceit.
- White-collar thefts include embezzlement (purposeful misappropriation of property entrusted to one's control, to which one is not entitled); extortion (purposely obtaining property from another person with that person's consent, when that consent is induced through wrongful use of force or official authority); forgery (falsely making or altering an official document with intent to defraud); and fraud (purposely obtaining the property of another person through deception).
- Offenses against public administration include bribery (the voluntary giving or receiving of anything of value with the intent of influencing a public official), obstruction of justice (intentional prevention of a public servant from performing an official function), official misconduct (unauthorized exercise of an official function with intent to benefit or injure another), and perjury (false swearing).
- Regulatory offenses, or corporate crimes, include administrative offenses (failure to comply with court orders or agency requirements), environmental violations (emissions or dumping in violation of legal standards), labor violations, manufacturing violations, and unfair trade practices.
- Arrest trends and demographic factors suggest that white-collar crime will increase in the future.

WHY IS COMPUTER CRIME A GROWING THREAT?

- Computers are the instrument in several types of crime. The most common of these is theft by computer.
- Other types of instrumental computer crime include use of a computer for harassment or extortion.
- Crimes in which computers are the object of the criminal act include causing damage to hardware or software, stealing trade secrets, and altering data for an unlawful purpose.
- As computers proliferate and computer literacy increases, rates of computer crime can be expected to increase as well.

HOW DOES ORGANIZED CRIME OPERATE?

- Organized crime is a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through the use of force, threats, monopoly control, and/or the corruption of public officials.

- In contrast to white-collar crimes, which generally occur as a deviation from legitimate business activity, organized crime takes place through a continuing criminal enterprise that exists to profit primarily from crime.
- The main types of organized crime are provision of illicit services (loan-sharking, prostitution, gambling), provision of illicit goods (drug dealing, fencing of stolen property), and infiltration of legitimate business (demands for “protection” money or no-show jobs).
- Research findings show that organized crime is not structured according to ethnic groups; rather, organized crime groups evolve around specific illicit activities.
- The true extent of organized crime is unknown, although there have been large increases in arrests for certain types of crime.
- Greater ease of travel and communication has made the commission of organized and transnational crime much easier.
- Among the most significant types of international crime are importation of stolen vehicles, drug smuggling, and illegal immigration.

WHAT ARE THE IMPACTS OF TERRORISM AND HATE CRIMES?

- Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
- Hate crimes are similar to terrorist acts except that a particular minority group (defined by race, ethnicity, nationality, or sexual orientation) is usually the target.
- There has been a general decline in the number of terrorist incidents since the 1980s, but those that are still being committed are becoming more deadly.

KEY TERMS

conspiracy 104	official misconduct 108
white-collar crimes 104	perjury 108
crimes of fraud 104	corporate crimes 108
crimes against public administration 104	computer crime 112
regulatory offenses 104	identity fraud 115
embezzlement 106	organized crime 116
extortion 106	racketeering 117
forgery 106	money laundering 117
fraud 107	crime syndicate 120
bribery 107	transnational crime 121
obstruction of justice 108	terrorism 125
	hate crimes 125

QUESTIONS FOR REVIEW AND DISCUSSION

1. What characteristics are common to all types of sophisticated crimes?
2. What factors must be present for conspiracy to be established?
3. What are the three main types of white-collar crime? Give an example of each.
4. Why is there reason to believe that white-collar crime will increase in the future?

5. In what kinds of crimes are computers the instrument? In what kinds are computers the object?
6. What is organized crime?
7. Give examples of each of the three basic types of organized crime.
8. What connection, if any, is there between organized crime and ethnicity?
9. What are some major types of international crime?
10. How is transnational drug smuggling carried out?
11. What is the distinction between terrorism and hate crimes?

NOTES

1. Edward Iwata and Elliot Blair Smith, "Skilling's Fall from Grace Comes to This," *USA Today* (February 20, 2004), p. 1B; "Senior Enron Figure Admits Insider Trading," *Facts on File World Digest* (October 30, 2003); "Waksal Gets 7-Plus Years," *CNN.com* (June 10, 2003); "Closing Arguments Underway," *CNN.com* (March 1, 2004); Paula Dobbyn, "Royal Caribbean to Pay Alaska \$3.5 Million in Dumping Charges" *Knight Ridder/Tribune Business News* (January 17, 2000); Reuters, "Royal Caribbean to Plead Guilty on Dumping Charges," *New York Times* (July 21, 1999), p. 1.
2. James D. Calder, "Al Capone and the Internal Revenue Service: State-Sanctioned Criminology of Organized Crime," *Crime, Law and Social Change* 17 (1992), pp. 1–23; Laurence Bergreen, *Capone: The Man and the Era* (New York: Simon & Schuster, 1994).
3. Jay S. Albanese, *White-Collar Crime in America* (Englewood Cliffs, NJ: Prentice Hall, 1995).
4. Adapted from *Proceedings of the Academic Workshop* (Morgantown, WV: National White Collar Crime Center, 1996).
5. Andrew Murr, "Living High on the Hog," *Newsweek* (October 27, 1997), p. 48.
6. John M. Caher, *King of the Mountain: The Rise, Fall, and Redemption of Chief Judge Sol Wachtler* (Buffalo: Prometheus Books, 1998); Bethany Kandel, "Top N. Y. Judge Faces Charges," *USA Today* (November 9, 1992), p. 2.
7. Kevin Johnson, "Probe Focuses on Online Sales of Fake Federal Ids," *USA Today* (May 26, 2000), p. 3A.
8. "Mount Pleasant Suit," *USA Today* (February 28, 1992), p. 8; "Porn Site, 900-Number Purveyors Settle FTC Fraud Charges," *Newsbytes* (January 31, 2002).
9. Tom Lowry, "American Family to Settle," *USA Today* (March 13, 1998), p. 1B; Tom Lowry, "Settlement Won't End American Family Woes," *USA Today* (March 20, 1998), p. 1B.
10. Joseph Stedino with Dary Matera, *What's in It for Me?* (New York: HarperCollins, 1993); Mark Mayfield, "S. Carolina Bribery Scandal Widens," *USA Today* (March 21, 1991), p. 4.
11. "Bribery Plea," *USA Today* (February 20, 1991), p. 5.
12. Albanese, *White-Collar Crime in America*, pp. 47–51.
13. Jacques Steinberg, "Scars in a Proud Police Force," *New York Times* (October 12, 1993), p. B1.
14. Associated Press, "Cleveland Judge Accused of Bribes," *New York Times* (March 2, 2000), p. 1.
15. Aaron Epstein, "Poindexter Guilty on All Counts," *Buffalo News* (April 8, 1990), p. 1.
16. "Cop Scandal May Affect 3,000 Cases," *New York Times* (December 15, 1999).
17. "Equifax Settlement," *USA Today* (July 1, 1992), p. 1B.
18. "Bayer to Pay \$1 Million over Advertising Claim," *New York Times* (January 12, 2000) p. A21.
19. Lorraine Woellert "Finally, an Enron Conviction," *Business Week* (September 11, 2003).
20. "Ypsilanti Man Gets 3 Years for Dumping Chemicals," *Associated Press* (February 12, 2004).
21. "Chicken Plant Executives Charged in Deadly Fire," *USA Today* (March 10, 1992), p. 3.
22. "Big Contractor Cited for Safety Violation," *Providence Business News* 14 (October 18, 1999), p. 16.
23. Stacey Schultz, "A Big Fat Settlement," *U.S. News & World Report* (October 18, 1999), p. 74; Paula Kurtzweil, "Sticking Public with Impure Products Puts Syrup Makers in Prison," *FDA Consumer* 31 (April 1997), p. 30.
24. "Baby Food Companies Fixed Price, Florida Says," *USA Today* (January 4, 1991), p. 3.
25. "Toys R Us, 2 Toy Makers to Pay \$50 Million in Cash, Toys in Suit," *Richmond Times-Dispatch* (May 26, 1999), p. C1.
26. Edward Cornish, "92 Ways Our Lives Will Change by the Year 2025," *The Futurist* (January–February 1996), pp. 1–15; David E. Bloom and Adi Brender, "Labor and the Emerging World Economy," *Population Bulletin* 48 (October 1993), pp. 2–39.
27. U.S. Bureau of the Census, *Statistical Abstract of the United States*, 116th ed. (Washington, DC: U.S. Government Printing Office, 1998), p. 14.
28. Tom Campbell, "6½ years, \$15 Million Payback Ordered in Theft," *Richmond Times-Dispatch* (April 6, 1999), p. 1.
29. Margaret Mannix, "Spammed and Scammed," *U.S. News & World Report* (May 31, 1999), p. 79.
30. Kim S. Nash, "PC Manager at Center of \$2 Million Grocery Scam: Inside Job Spotlights Critical Security Threat," *Computerworld* (March 30, 1998), p. 1.
31. Fred Bayles, "Computers Aid Amateur Counterfeiters," *USA Today* (May 11, 1999), p. 3.
32. Deborah Kong, "Internet Auction Fraud Increases," *USA Today* (June 23, 2000), p. 3B.
33. "Man on Most Wanted List Pleads Guilty to Hacking," *Richmond Times-Dispatch* (March 28, 1999), p. 2; Kathy Rebello, "'Sensitive Kid' Faces Fraud Trial," *USA Today* (February 28, 1989) p. 1B.
34. "Computer Security a Mess, Report Says," *USA Today* (December 6, 1990), p. 3; see also "Arrest in Hacking at NASA," *New York Times* (March 19, 1998), p. 19.

35. Mark Lewyn, "Computer Verdict Sets 'Precedent'," *USA Today* (September 21, 1988), p. 1.
36. Kathy Rebello and Leslie Werstein, "Brilliance Has Its Roots in Family Life," *USA Today* (November 10, 1988), p. 1B; Ted Eisenberg et al., "The Cornell Commission on Morris and the Worm," *Communications of the ACM* 32, no. 6 (June 1989), pp. 706-9; William Kates, "Cornell Student Convicted in Computer Case," *Buffalo News* (January 23, 1990), p. 3; Amy Harmon, "As Digital Vandals Disrupt the Internet, a Call for Oversight," *New York Times* (September 1, 2003), p. A1.
37. "Computer 'Bomb,'" *USA Today* (November 27, 1995), p. 3; "Man Arrested at Library for Extortion," *Library Journal* (Sept 15, 2000), p. 11.
38. Hoag Levins, "Hackers Devastate Texas Newspapers' Servers," *Editor & Publisher* (June 28, 1997), p. 45.
39. "Cyberwars," *USA Today* (April 24, 1998), p. 8.
40. "Bogus Software," *USA Today* (August 30, 1991), p. 1D.
41. Carroll Bogert, "Windows 95, 5 Bucks," *Newsweek* (May 26, 1997), p. 82.
42. Clifford Stoll, *The Cuckoo's Egg: Inside the World of Computer Espionage* (New York: Doubleday, 1989).
43. Brendan Koerner, "Can Hackers be Stopped?," *U.S. News & World Report* (June 14, 1999), pp. 46-52.
44. Laura DiDio, "Computer Crime Costs on the Rise," *Computerworld* (April 20, 1998), p. 55; "Loss from Hack Attacks" *LA Times* (March 22, 2000), p. 5.
45. Koerner, "Can Hackers be Stopped?," pp. 46-52.
46. *Ibid.*
47. U.S. Comptroller General, *Identity Fraud* (Washington, DC: U.S. General Accounting Office, 1998); Margaret Mannix, "Getting Serious about Identity Theft," *U.S. News & World Report* (November 8, 1999), p. 88.
48. William F. Skinner and Anne M. Fream, "A Social Learning Analysis of Computer Crime among College Students," *Journal of Research in Crime and Delinquency* 34 (November 1997), pp. 495-519.
49. Wendy R. Leibowitz, "Low-Profile Feds Fashion Laws to Fight Cybercrime," *The National Law Journal* (February 2, 1998), p. 1.
50. Laura DiDio, "Special FBI Unit Targets Online Fraud, Gambling," *Computerworld* (April 27, 1998), p. 47.
51. Carol Levin, "Internet Capers," *PC Magazine* (October 21, 1997), p. 29.
52. President's Commission on Law Enforcement and Administration of Justice, *Task Force Report: Organized Crime* (Washington, DC: U.S. Government Printing Office, 1967), p. 33.
53. Jay S. Albanese, *Organized Crime in Our Times* (Lexis/Nexis/Anderson, 2004), p. 3.
54. National Advisory Committee on Criminal Justice Standards and Goals, *Report of the Task Force on Organized Crime* (Washington, DC: U.S. Government Printing Office, 1976), p. 213.
55. Henry N. Pontell and Kitty Calavita, "White-Collar Crime in the Savings and Loan Scandal," *The Annals* 525 (January 1993), p. 39.
56. See Albanese, *White-Collar Crime in America*.
57. President's Commission on Organized Crime, *The Impact: Organized Crime Today* (Washington, DC: U.S. Government Printing Office, 1987), pp. 33-128.
58. Alan A. Block, "The Snowman Cometh: Coke in Progressive New York," *Criminology* 17 (May 1979), pp. 75-99; President's Commission on Organized Crime, pp. 64, 81, 91.
59. Block, p. 95.
60. Patricia A. Adler, *Wheeling and Dealing: An Ethnography of an Upper-Level Drug Dealing and Smuggling Community* (New York: Columbia University Press, 1985), p. 80.
61. Peter Reuter, *Disorganized Crime: The Economics of the Visible Hand* (Cambridge, MA: MIT Press, 1983), p. 175-76.
62. Francis A. J. Ianni with Elizabeth Reuss-Ianni, *A Family Business: Kinship and Social Control in Organized Crime* (New York: New American Library, 1973), p. 20.
63. Joseph L. Albini, *The American Mafia: Genesis of a Legend* (New York: Irvington, 1971), p. 288.
64. See Jay S. Albanese, "Casino Gambling and Organized Crime: More Than Reshuffling the Deck," in Jay S. Albanese, ed., *Contemporary Issues in Organized Crime* (Monsey, NY: Willow Tree Press, 1995).
65. Kevin Johnson, "Cell Phone 'Cloners' Pushing the Law's Buttons," *USA Today* (June 21, 1996), p. 3.
66. Margaret Mannix, "Keeping a Check on Debit Card Liability," *U.S. News & World Report* (September 8, 1997), p. 7.
67. Richard Barnet and John Cavanagh, *Global Dreams* (New York: Simon & Schuster, 1995).
68. Jonathan M. Winer, "International Crime in the New Geopolitics: A Core Threat of Democracy," in William F. McDonald, ed., *Crime and Law Enforcement in the Global Village* (Cincinnati: Anderson, 1997), p. 41.
69. Carol J. Castaneda, "Car Thieves Wheeling and Dealing Overseas," *USA Today* (March 4, 1996), p. 3.
70. U.S. Comptroller General, *Efforts to Curtail the Exportation of Stolen Vehicles* (Washington, DC: U.S. General Accounting Office, 1999).
71. *Ibid.*
72. www.nicb.org (2003).
73. "Organized Crime and International Terrorism," *International Criminal Police Review*, vol. 472 (1998).
74. "Worldwide Nigerian Heroin Smuggling Ring Smashed," *Organized Crime Digest* (May 27, 1992), p. 3; "New Breed of Smugglers," *USA Today* (September 23, 1991), p. 3; "Nigerian Man Arrested for Heroin Smuggling," *Jakarta Post* (January 11, 2002).
75. U.S. Comptroller General, *Drug Control: Interdiction Efforts in Central America Have Had Little Impact on the Flow of Drugs* (Washington, DC: U.S. General Accounting Office, 2000).
76. Ko-lin Chin, *Smuggled Chinese: Clandestine Immigration into the United States* (Philadelphia: Temple University Press, 2000).
77. Sam Howe Verhovek, "Wretched Masses, Smuggled," *New York Times* (January 16, 2000), p. 2.
78. William F. McDonald, "Illegal Immigration: Crime, Ramifications, and Control (The American Experience)," in William F. McDonald, ed., *Crime and Law Enforcement in the Global Village* (Cincinnati: Anderson, 1997), pp. 65-88.
79. John Scalia, *Noncitizens in the Federal Justice System* (Washington, DC: Bureau of Justice Statistics, 1996); Norman J. Rabkin, *Criminal Aliens: INS' Efforts to Identify and Remove Imprisoned Aliens Need to be Improved* (Washington, DC: U.S. General Accounting Office, 1997).
80. Kit R. Roane, "North of the Border, Terror's 'club Med'," *U.S. News & World Report* (August 7, 2000), p. 46.

81. U.S. Department of Justice. *Assessment of U.S., Activities to Combat Trafficking in Persons* http://www.usdoj.gov/crt/crim/wetf/us_assessment.pdf (2003).
82. William F. McDonald, "Illegal Immigration," p. 83.
83. Federal Bureau of Investigation, *Terrorism in the United States, 1999* (Washington, DC: U.S. Government Printing Office, 2001), p. 2.
84. Michael Janofsky, "Man Is Convicted in Killing of Gay Student," *New York Times* (November 4, 1999), p. A14.
85. Benjamin Weiser, "'Mastermind' and Driver Found Guilty in 1993 Plot to Blow Up Trade Center," *New York Times* (November 13, 1997), p. 1; Gary Fields, "Yousef Sentenced to 240 Years in Solitary," *USA Today* (January 1, 1998), p. 4.
86. David E. Kaplan and Mike Tharp, "Terrorism Threats at Home: Two Years after Oklahoma City, Violent Sects Still Abound," *U.S. News & World Report* (January 5, 1998), pp. 22–27.
87. Warren P. Strobel, Kit R. Roane, Chitra Ragavan, "The Case of the Strange Conspiracy," *U.S. News & World Report* (January 17, 2000), p. 27.
88. Federal Bureau of Investigation, *Hate Crime Statistics* (Washington, DC: U.S. Government Printing Office, 2002).
89. *U.S. v. Winslow, Nelson, and Baker*, 962 F. 2d 845 (9th Cir. 1992) at 849.
90. *Ibid.*
91. *Ibid.*, and also *United States v. Stauffer*, 922 F. 2d 508 (9th Cir. 1990) at 514–15.
92. Gordon Witkin and Ilan Greenberg, "End of the Line for the Unabomber," *U.S. News & World Report* (February 2, 1998), p. 34; Ted Gest, "End of the Line," *U.S. News & World Report* (May 18, 1998), p. 37.
93. Gest, p. 11; Brent L. Smith, *Terrorism in America: Pipe Bombs and Pipe Dreams* (Albany, NY: State University of New York Press, 1994), p. 198–99.
94. "The Real Battle," *U.S. News & World Report* (April 27, 1998), p. 7; U.S. Comptroller General, *Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy* (Washington, DC: U.S. General Accounting Office, 1997); U.S. Comptroller General, *Terrorism and Drug Trafficking: Responsibilities for Developing Explosives and Narcotics Detection Technologies* (Washington, DC: U.S. General Accounting Office, 1997).
95. U.S. Comptroller General, *Combating Terrorism: Issues to be Resolved to Improve Counterterrorism Operations* (Washington, DC: U.S. General Accounting Office, 1999); U.S. Comptroller General, *Combating Terrorism: Federal Response Teams Provide Varied Capabilities* (Washington DC: U.S. General Accounting Office, 2002).
96. National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Washington, DC: U.S. Government Printing Office, 2000).
97. Jonathan R. White, *Defending the Homeland* (Belmont, CA: Wadsworth, 2004).