# CHAPTER 18
# **Cyber Crime**
*Clay Wilson*

CYBER CRIME is becoming a highly organized underground business on the Internet, where criminals advertise a variety of disruptive software products and malicious technical services for sale or rent. High-end cyber crime groups use modern business practices to keep their software products updated with the latest antisecurity features while seeking to recruit new software engineering talent into their organizations. Cyber criminals use the Internet to direct large networks of remotely controlled "zombie" computers to attack in swarms, attempting to infect additional computers, distribute unwanted spam, or deny Internet access and services to legitimate users. Attribution of cyber crime to perpetrators is problematic, and new technologies outpace law enforcement capabilities. As malicious code grows in sophistication and the consequences of cyber crime expand, this emerging threat to national security may also alter discussions about cyber terrorism.[1]

This chapter begins by describing the characteristics of cyber crime and offering examples of how it has evolved over the past few years. Next is a discussion of the tools of cyber crime, such as botnets, malicious code on Web sites, and identity theft, which has also been linked to terrorist activity. An examination of cyber espionage shows how Internet technology has caused a dilemma: this form of "cyber crime" may also be viewed as a necessity in business competition or maintenance of national security. Discussion includes insider threats, piracy of intellectual property, and money laundering (especially associated with drug traffickers).

The next section describes law enforcement issues, including problems in measuring the scope and economic effects of cyber crime and in tracing evidence associated with a cyber crime. The problem is addressed but not solved by the Convention on Cybercrime, the first international agreement to coordinate the work of cyber crime law enforcement agencies in different countries.

The chapter then examines organized crime, which is increasing its operations in cyberspace, and the future of organized cyber crime, including potential attacks on infrastructure control systems and links with terrorism.

The chapter ends by encouraging decisionmakers to pay more attention to the urgent need for improvements to cyber security. The conclusion presents crucial policy questions and warnings (in particular, the possibility that extremists can now employ sophisticated cyber crime tools for cyber terrorism without the need to develop their own hard-to-obtain technical skills).

## *Characteristics of Cyber Crime*

Cyber crime is usually enabled and conducted through a connection to the Internet but can also involve unauthorized removal of data on small, portable storage devices (known as flash drives or thumb drives). Crime in cyberspace can be committed anonymously with relative ease and sometimes even can occur without detection by the victim. Cyberspace allows criminals to extend their reach across national borders, putting at risk a wider population of potential victims. Consumers who use new "Web 2.0" tools for sharing data on social networking Web sites such as MySpace and YouTube, and on business networking Web sites such as LinkedIn, are increasingly at risk as criminals capture personal information and corporate data for purposes of fraud and extortion.[2] Problems of coordination among law enforcement agencies of different countries, and sometimes conflicting national policies about crime in cyberspace, combine to aid cyber criminals who may choose to operate from geographic locations where penalties for some forms of cyber crime may not yet exist.

The possibility of illicit profits, together with a low probability of detection or identification, can make cyber crime attractive. Criminal groups that lack the technical skills needed to manipulate computer code may hire the services of individual (or groups of) hackers. Profitable alliances of hackers and criminals can be rapidly created as needed and then just as quickly dissolved. Where illicit profits are potentially large, some criminal groups have adopted standard information technology (IT) business practices to systematically develop more efficient and effective computer code for cyber crime. Cyber criminals reportedly now sell or rent software products in online markets for customers to use to support their own cyber crimes. For example, some security experts suspect that such services may have been used in the April 2007 attack in Estonia (discussed below). When illicit profits become the only concern, it is possible that future customers of cyber criminals may comprise anyone who can pay for services, possibly including terrorist groups.

Some argue there is no agreed definition for *cyber crime* and that *cyberspace* is just a new instrument used to commit crimes that are not new at all. For example, cyber crime may involve theft of intellectual property in violation of existing patent, trade secret, or copyright laws. Press releases on the U.S. Department of Justice's Web site indicate the variety of activities that fit into the category of cyber crime:[3]

- "'Phisher' Sentenced to Nearly Six Years in Prison after Nation's First Can- Spam Act Jury Trial Conviction" (June 14, 2007)
- "Man Indicted for Illegally Transmitting Electronic Funds from Various Banks to Ameritrade and E*Trade, Totaling Approximately $3,348,000.00" (May 9, 2007)
- "Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting" (April 27, 2007)
- "Man Charged with Computer Fraud and Aggravated Identity Theft: Internet 'Phishing' Scheme Used to Steal Thousands of Credit and Debit Card Numbers, Social Security Numbers" (April 26, 2007)
- "Couple Charged with Criminal Copyright and Trademark Violations for Distributing Counterfeited Microsoft Software" (June 12, 2007)
- "Man Sentenced to Five Years in Prison for Conducting a Multi-Million Dollar International Cable Piracy Business" (June 8, 2007)
- "Former Computer Contractor Pleads Guilty to Hacking Daimler Chrysler Parts Distribution Wireless Network" (June 1, 2007)
- "Man Charged with Leaking Season Premier of Popular Television Show by Uploading to the Internet" (June 1, 2007)
- "Ex-Employee of the Coca Cola Company and Co-Defendant Sentenced for Stealing Trade Secrets" (May 23, 2007)
- "Software Piracy Crackdown 'Operation Fastlink' Yields 50th Guilty Plea" (May 14, 2007)
- "Man Receives Federal Sentence for Copying Copyrighted Movies" (May 11, 2007).

### *Evolution of Cyber Crime*

Most cyber crime has taken the form of massive, widespread attacks intended to affect all users of the Internet. Increasingly, however, cyber crime involves the use of remotely controlled software that can focus the power of many hacked zombie computers to attack a specific target. Thousands of individual computers infected with malicious code are remotely directed via the Internet to attack in swarms, called *botnets*. Two examples illustrate how cyber crime has evolved from randomly targeted attacks to sophisticated, controlled attacks focused on specific targets. The first example describes a single Internet worm that, in 2005, spread randomly to infect thousands of computers worldwide.

An 18-year-old Moroccan national and a 21-year-old resident of Turkey were arrested in 2005, and sentenced in 2006, for creating and spreading computer worms that disrupted services on computer networks of major U.S. news organizations and other institutions during August 2005. The Zotob worm and its variants were designed to remotely instruct computers to send email spam, steal personal data, or attack other computers without the user's knowledge. According to Federal Bureau of Investigation (FBI) Assistant Director Louis Reigel, who at the time headed the cyber division, investigators believe the malicious code was created by one hacker and sold to the other hacker for financial gain. The Zotob worm was an example of a widespread cyber attack that did not show evidence of specific targets for identity theft, bank fraud, or forgery. It is estimated to have cost $500 million in lost productivity and other nuisance damage to many corporate and individual users.[4]

The Zotob incident was an example of the type of widespread and random cyber attack in which hackers seemed to be looking less for monetary gain than for notoriety. Subsequently, however, Department of Justice officials indicated they were observing a change in the apparent motives of people who attack computer networks away from bragging rights and toward monetary motives.[5] Now, cyber crime is apparently becoming a fee-for-service business operation, where criminals offer technical skills and malicious code products for sale or rent. Such an arrangement may be behind a recent cyber attack that involved thousands of computers worldwide simultaneously attacking government computer systems in Estonia.

On April 27, 2007, officials in Estonia relocated a Soviet-era war memorial commemorating an unknown Russian who died fighting the Nazis, and the move stirred emotions. Ethnic Russians in Estonia rioted, and the Estonian embassy in Moscow was blockaded. Several large and sustained distributed denial-of-service (DDOS) attacks were launched against many Estonian national Web sites, including those of government ministries and the prime minister's Reform Party.[6] The attacks, which flooded computers and servers and blocked legitimate users, were described as crippling to Estonia's limited resources for support of its communications infrastructure.

As in any cyber attack, accurate identification of the attacker was difficult. This uncertainty means that it is difficult to name a target for retaliation (which in turn affects deterrence, as discussed in chapter 13 in this volume, "Deterrence of Cyber Attacks"), and creates uncertainty over whether a retaliatory or other response should come from law enforcement or the military. In the Estonia case, the North Atlantic Treaty Organization and the United States sent computer security experts to Estonia to help recover from the attacks, analyze the methods used, and attempt to determine their source.

Initially, some Estonian officials blamed the Russian government for the cyber attacks and even made charges of cyberwarfare. Other observers linked the cyber attacks to transnational cyber criminals who had made large botnets available for short-term rent. It was noted that as the rented time expired, the intensity of the persistent cyber attacks against Estonia also began to fall off.[7] However, not all security experts agree, and it remains unclear whether the cyber attacks were sanctioned or initiated by the Russian government or a criminal botnet was involved.

Some network analysts later concluded that the cyber attacks targeting Estonia were not a concerted attack but instead were the product of spontaneous anger from a loose federation of separate attackers. Technical data showed that sources of the attack were worldwide rather than concentrated in a few locations. The computer code that caused the DDOS attack was posted and shared in many Russian-language chat rooms, where the moving of the war memorial was an emotional topic. These analysts stated that although access to various Estonian government agencies was blocked by the malicious code, there was no apparent attempt to target national critical infrastructure other than Internet resources, and no extortion demands were made. Their analysis led them to believe that there was no Russian government connection to the attacks against Estonia.[8] However, investigation into the incident continues, and U.S. officials view some aspects of the event as a possible model for future cyber attacks against other nation-states. In February 2008, an Estonian court convicted a 20-year-old ethnic Russian living in Estonia of participating in the cyber attack and ordered him to pay a fine of €1,120. To date, this is the only conviction associated with the cyber attack.[9]

Cyber crime, and the accompanying publicity, has given some practitioners a celebrity status within the hacking community. Authors of malicious code now collaborate to produce annual conferences and seminars where hacking methods are showcased and potential security vulnerabilities are publicly exposed.[10] Organized crime groups are also actively recruiting skilled IT students into cyber crime. These recruits include college graduates and technical expert members of computer societies, who might be sponsored to attend IT courses to further their technical expertise. However, in some cases, the targeted student may not realize that a criminal organization is behind the recruitment offer or the support for their education.[11]

Anonymity is part of another recent trend, as cyber attacks are increasingly designed to silently steal information without leaving behind any damage that a user would notice. These types of attacks are designed to escape detection in order to remain on host systems for longer periods of time. Cyber criminals can also work out in the open, rather than in their basements, because the pervasiveness of the Internet helps maintain anonymity. For example, Internet cafes often clean their computers by automatically rebooting and wiping all nonstandard files between each customer.

Cyber criminals post update information about their computer exploits as a type of advertising, so their business customers can be sure they purchase the latest malicious code with new features to elude newer commercial antivirus tools. Criminals put legitimate Web sites where Web crawlers will inspect them, but innocent users who later visit the site are routed to infected sites.[12] Another trick is to customize the malicious code so that each visitor to an infected Web site is infected by a differently encrypted version of the code; this helps defeat newer antivirus tools. Thus, criminals can evade detection while continuing to spread malicious code.

Counterfeit software is sold to U.S. and foreign consumers with features that facilitate later infections by computer viruses. Sale of counterfeit goods is on the increase as eBay and similar Web sites gain prominence outside the United States in countries where laws are unsettled or are unfavorable to U.S. crime victims.

Criminals use “phishing” techniques, masquerading as a trustworthy entity in an attempt to acquire sensitive information for fraudulent purposes. Phishing is typically carried out by an email or instant message requesting that recipients respond with user names, computer passwords, and credit card or banking details, or that they expose sensitive information by visiting a Web site. Users of eBay, online banks, and investment services are common targets. Criminals also use the services of popular payment networks such as PayPal and E-Gold for money laundering and masking illegal activities. Some cyber criminals may engage in cyber crime to finance terrorist schemes (discussed further below; also see chapter 19 in this volume, “Cyber Terrorism: Menace or Myth?”).[13]

## Tools of Cyber Crime

Increasing in use are botnets, malicious code on Web sites, identity theft, cyber espionage, theft or abuse of insider information, piracy and trade in counterfeit goods, and money laundering.

### *Botnets*

*Bot* (from *robot*) *networks* or *botnets* are made up of vast numbers of computers that are infected and remotely controlled to operate, in concert, through commands sent via the Internet. They are used to block or disrupt the computers of targeted organizations or to distribute spam, viruses, or other malicious code. Botnets have been described as the “Swiss Army knives of the underground economy” because they are so versatile.

Jeanson Ancheta, a young hacker and member of a group called the “Bot- master Underground,” reportedly made more than $100,000 from Internet advertising companies who paid him to download their malicious “adware” code onto more than 400,000 vulnerable personal computers (PCs) he had secretly taken over.[14] He also made tens of thousands of dollars renting his 400,000-unit “botnet herd” to companies that used it to send out spam, viruses, and other malicious code on the Internet. In 2006, Ancheta was sentenced in U.S. District Court in California to nearly 5 years in prison after pleading guilty under an indictment for conspiring to violate the Computer Fraud Abuse Act; conspiring to violate the Controlling the Assault of Non-Solicited Pornography and Marketing Act; causing damage to computers used by the Federal Government in national defense; and accessing protected computers without authorization to commit fraud, in the first U.S. case to target profits derived from use of botnets.[15]

Botnet code was originally distributed as infected email attachments. When users click to view a spam message, botnet code can be secretly installed on their PC. As users have grown more cautious, cyber criminals have turned to other methods. A Web site may spread infection by means of an ordinary-looking advertisement banner or a link to an infected Web site. Clicking on any of these may install botnet code. Botnet code can be silently uploaded, even if the user takes no action while viewing the Web site, if the browser has certain unpatched vulnerabilities. Firewalls and antivirus software do not necessarily inspect all data that is downloaded through browsers, and some bot software can disable antivirus security.

Once a PC has been infected, the malicious software (or *malware*) establishes a secret communications link to a remote botmaster or bot-herder by which it receives commands to attack a specific target. The malicious code may also automatically probe the infected PC for personal data or may log keystrokes and transmit the information to the botmaster.

The Shadowserver Foundation monitors the number of bot networks being controlled online at any given time by monitoring command-and-control servers. From November 2006 through May 2007, it found approximately 1,400 active command-and-control servers. The number of individual infected drones or zombies controlled by such servers reportedly grew from half a million in March 2007 to more than 3 million in May 2007. Symantec, another security organization, reported that it detected 6 million bot-infected computers in the second half of 2006.[16] Some botnet owners reportedly rent out huge networks for $200 to $300 an hour. Botnets are increasingly used for fraud and extortion.[17]

Newer methods for distributing bot software may complicate law enforcement efforts to identify and locate the originating botmaster. Authors of software for Botnets are increasingly using modern open-source techniques for software development, including use of multiple contributors to the design, new releases that fix bugs in the malicious code, and modules that make portions of the code reusable for newer malicious software. This behavior mirrors the code development techniques used to create commercial software products and is expected to make future botnets more robust and reliable, making malware more attractive to criminals.[18]

### *Malicious Code Hosted on Web Sites*

Users who lacked important software security patches and who visited the popular MySpace and YouTube Web sites in 2005 may have had their PCs infected. If they clicked on a particular banner advertisement, it silently installed malicious code on their computers to log keystrokes or capture sensitive data. During the first half of 2006, the Microsoft Security Team reported that it removed 10 million pieces of malicious software from nearly 4 million computers and Web servers.[19] When analysts at Google examined several million Web pages for the presence of malicious software, they determined that 4.5 million of the Web pages examined were suspicious in nature. After further testing of those pages, over 1 million were found to launch downloads of malicious software, and more than two-thirds of those programs were bot software that, among other things, collected data on banking transactions, which it emailed to a temporary (and thus hard to trace) email account.[20]

Researchers at Finjan, Inc., a California security firm, reviewed security data from the first quarter of 2007. Based on an analysis of more than 10 million unique Web sites from Internet traffic, they found that attacks are increasingly using code obfuscation through diverse randomization techniques, making them almost invisible to pattern-matching or signature-based methods in use by traditional antivirus products; and that more and more, malicious code is embedded within legitimate content, with less dependence on outlaw servers in unregulated countries. Finjan found that 90 percent of the Web sites it examined that contained malware resided on servers located in the United States or the United Kingdom.[21] This finding contradicts the common perception that malicious code is primarily hosted in countries where e-crime laws are less developed.

### *Identity Theft*

Individual users may become victims of cyber crime if they are lured into clicking on tempting links in email or on Web sites, such as offers to “buy Rolex watches cheap” or “check out my new photos.” These links might be configured to place malicious software onto a user’s system by exploiting Web browser vulnerabilities.

Malicious code placed in this way can scan a victim's computer for sensitive information, such as name, address, telephone number, place and date of birth, Social Security number, and answers to commonly used security questions such as mother's maiden name. Identity information obtained this way is then sold in online markets. Purchasers might use it to create false identity documents: readily available equipment such as a digital camera, color printer, and laminating device might be used to make official-looking driver's licenses, birth certificates, reference letters, or bank statements.[22]

Inadequate computer security practices within organizations sometimes facilitate identity theft involving thousands of victims. Over 218 million records containing sensitive personal information were involved in U.S. security breaches between January 2005 and March 3, 2008. For example, on February 27, 2008, 103,000 individual records were compromised when personal information, including Social Security numbers, for thousands of doctors in 11 states was openly posted on a company Web site.[23] In June 2006, officials from the U.S. Department of Energy acknowledged that personal information belonging to more than 1,500 employees of the National Nuclear Security Administration had been stolen in a network intrusion that apparently took place starting in 2004 and was not discovered until a year later.[24]

Stolen credit card numbers and bank account information are now traded online in a highly structured arrangement involving buyers, sellers, intermediaries, and service industries. Services offered include changing the address of a stolen identity through manipulation of stolen personal identification numbers or passwords. Some observers estimated that in 2005, such services for each stolen MasterCard number cost between $42 and $72.[25] The cost has apparently gone down: other studies show that in 2007, a stolen credit card number would sell online for $1, while an identity complete with U.S. bank account number, credit card number, date of birth, and government-issued ID number sold for $14 to $18.[26]

### *Cyber Espionage*

*Cyber espionage* involves the unauthorized probing of a target computer's configuration to evaluate its system defenses or the unauthorized viewing and copying of data files. If a terrorist group, nation, or another organization uses computer hacking techniques for political or economic motives, such intrusions could be criminal. If there is disagreement about this, however, it is because technology has outpaced policy in cyberspace. In some views, industrial cyber espionage is considered a necessary part of global economic competition, and secret monitoring of the computerized functions and capabilities of potential adversary countries may be considered essential for national defense.

In 2001, a special committee of inquiry established by the European Parliament accused the United States of using a Cold War–era electronic spy network to engage in industrial espionage against European businesses.[27] The United States set up the Echelon network in 1971; Britain helps operate the system, and there are listening posts in Canada, Australia, and New Zealand. Echelon is described as a global spy system capable of intercepting phone calls, electronic mail, and fax messages made from almost any location around the world. The European Parliament charged that information gathered on Echelon helped the United States beat the European Airbus Consortium in selling aircraft to Saudi Arabia in 1994. The State Department denied that the U.S. Government was engaged in industrial espionage. However, the former director of the Central Intelligence Agency, James Woolsey, reportedly justified the possibility of doing so on the basis that European companies use bribery. This prompted an outraged response from officials of the European Parliament, but no denial that companies sometimes used bribery to secure a deal.[28]

Reliance on technology has changed the nature of both military and industrial espionage, and the Internet offers new low-cost and low-risk opportunities for espionage. Some government officials warn of an increased risk to U.S. national security due to cyber espionage by other countries since criminals now sell or rent malicious code tools to conduct it. One industry official, arguing for stronger government agency computer security practices, stated, "If gangs of foreigners broke into the State or Commerce Departments and carried off dozens of file cabinets, there would be a crisis. When the same thing happens in cyberspace, we shrug it off as another of those annoying computer glitches we must live with."[29]

In 2003, a series of computer attacks designed to copy sensitive data files was launched against Department of Defense (DOD) systems and computers belonging to DOD contractors. The cyber espionage attack apparently went undetected for many months. DOD suspected that this series of cyber attacks, later labeled Titan Rain, originated in China. The attacks were directed against the Defense Information Systems Agency, the Redstone Arsenal, the Army Space and Strategic Defense Installation, and several computer systems critical to military logistics. Although no classified systems were breached, many files were copied containing sensitive information that is subject to U.S. export-control laws.

In 2006, an extended computer attack against the U.S. Naval War College in Newport, Rhode Island, prompted officials to disconnect the entire campus from the Internet.[30] A similar attack against the Pentagon in 2007 led officials to temporarily disconnect part of the unclassified network from the Internet.[31]

Accurate attribution is important when considering whether to retaliate using military force or police action. DOD officials suspect that the majority of cyber attacks against DOD and U.S. civilian agency systems originated in China, and these attacks are consistently more numerous and sophisticated than cyber attacks from other malicious actors.[32] The motives appear to be primarily cyber espionage against civilian agencies, DOD contractors, and DOD systems. The espionage involves unauthorized access to files containing sensitive industrial technology and unauthorized research into DOD operations. Some attacks included attempts to implant malicious code into computer systems for future use by intruders.[33]

Security experts warn that all U.S. Federal agencies should now be aware that some malicious actors in cyberspace make no distinction between military and civilian targets. According to an August 2005 computer security report by IBM, more than 237 million overall security attacks were reported globally during the first half of that year.[34] Government agencies were targeted the most, reporting more than 54 million attacks, while manufacturing ranked second (36 million), financial services ranked third (around 34 million), and then health care (over 17 million). The United States was the most frequent target, with 12 million attacks in the first half of 2005 on U.S. Government agencies and industries, followed by New Zealand (1.2 million) and China (1 million). Moreover, the number of incidents reported is only a small fraction of the total number of attacks that actually occur.

### *The Insider Threat*

A major threat for organizations is the ease with which data can be copied and carried away using small storage devices such as thumb drives. Future advances in technology that allow installed computer applications to be run entirely from the thumb drive mean that the entire contents of a PC might be copied to a small, portable, easily concealed device.[35]

A 2003 study of security incidents conducted by the U.S. Secret Service and the Carnegie Mellon Software Engineering Institute found that attacks on computer systems committed by insiders with authorized access have cost industry millions of dollars in fraud and lost data.[36] Insider employees with access to sensitive information systems can initiate threats by inserting malicious code into software as it is being developed, either locally or under offshore contracting arrangements. The risk is suggested by the January 2003 arrest and eventual conviction of 20 employees of subcontractors working in the United States at the Sikorsky Aircraft Corporation; they were charged with possession of false identification, which they had used to obtain security access to facilities containing restricted and sensitive military technology.[37]

### *Piracy and Counterfeit Goods*

Anything that can be digitized can be transmitted rapidly through the Internet from one computer to another, with no reduction of quality for second-generation or subsequent copies. *Piracy* is the term used to describe theft of intellectual property, or the illegal copying of software, music, movies, and other digital items protected by copyright, trade secret, or patent laws.

The U.S. State Department cites data that show global losses from piracy of creative works and software at $30 billion–$35 billion per year.[38] Some estimate that up to 92 percent of all computer software currently used in mainland China is counterfeit.[39] Theft of intellectual property affects the entire U.S. economy, through lost employment and taxes, as well as the economies of all countries that protect digital products. Sources in Europe estimate that economic losses related to counterfeiting are around €500 billion per year. Additionally, some counterfeit food or medical products present a serious health threat.[40] Concerns over digital piracy are rising as terrorist groups collaborate with cyber criminals trafficking in counterfeit goods, products, and intellectual property, activities potentially even more lucrative than drug trafficking. Former Attorney General Alberto Gonzales noted that this is "more than just a question of protecting IP [intellectual property], it's a question of [national] security."[41]

Pirated digital copies of copyrighted work transmitted over the Internet are sometimes known as *warez*, and *warez groups* illegally copy and distribute hundreds of millions of dollars' worth of copyrighted material each year. Pirated trade secrets are sold to other companies or to criminal groups who use the information to extort money from legitimate companies. Pirated software is sold at prices that undercut legitimate digital products. It is especially vulnerable to attack from malicious code because important security patches and updates distributed by the legitimate software company are never installed.

### *Money Laundering*

In April 2007, the E-Gold company was indicted by the U.S. Government for money laundering.[42] E-Gold is one of a number of Internet services that allow users to deal in shares of precious metal and avoid government tracking of currency. E-Gold was started in 1996 as one of several pioneer Internet Web payment systems that converted different forms of conventional money into a form of digital Web currency. E-Gold was intended to become an easily accepted, independent currency that would enable persons from countries all over the world to exchange products at stable prices and without the negative effects of inflation usually associated with government paper money. Customers of E-Gold were not required to prove their identities, so they were able to use false names when opening an account. By using a wire transfer, a credit card, or a digital cash card, a customer would buy units of E-Gold and could transfer them to anyone else with an E-Gold account, exchange E-Gold units for regular money, or transfer E-Gold value onto a portable digital cash card. Banks are legally required to monitor customers and report suspicious transactions to the

U.S. Government, but E-Gold is not bound by these regulations, and therefore it attracted online criminals who wanted to move money quickly without detection. Reportedly, the cyber crime group known as ShadowCrew was one of several suspicious groups that used E-Gold to launder money in 2004.[43] Many Web sites that sell stolen bank account and credit card information or that deal in child pornography requested payment via E-Gold. However, E-Gold reportedly cooperated with watchdog organizations, such as the National Center for Missing and Exploited Children, in attempts to crack down on payment schemes used by child pornography Web sites.[44]

Other electronic payment services also let users operate accounts anonymously, sometimes using only phone cards for identification. These Internet payment services closely resemble the money-changing system known as *hawala* that has been used by Middle Eastern terrorists. A customer gives money to a *hawala* service located in one area; that service telephones a similar service located in another city or country, which gives out money to a designated recipient. Some terrorism experts believe that terrorist groups increasingly will use Internet payment services to move funds without government detection.[45]

Virtual casinos, Internet auctions, online banking, and the sale of shares, bonds, and futures online also offer ample opportunities for money laundering.[46] Internet gambling is reportedly a $12-billion-a-year industry that relies heavily on international online payment services. Many U.S. credit card companies started refusing to process gambling transactions in 2001, and U.S. law now bars financial institutions from processing illegal gambling transactions. However, it would be difficult for the United States, or any other country, to prohibit the processing of financial transactions that are legal in the nation from which a business operates. It is also problematic for U.S. law enforcement to stop Internet payment services from processing illegal gambling transactions made from U.S. computers. Cyber criminals continue to exploit numerous advantages arising from such differences in jurisdictions.[47]

Other methods for money laundering include the use of "e-purses" such as smart cards that store and transport funds in memory chips. Internet payment services, such as PayPal and Neteller, operate outside traditional banks or credit card companies. Neteller was said to process over $5 billion in transactions in 6 months in 2006.[48] In May 2007, 143 million consumers reportedly had PayPal accounts, and PayPal "handled more than $11 billion in payments through all its services in the first quarter of 2007, up 30% from a year ago."[49]

Another method uses "money mules," individuals who are hired to assist international wire fraud and other illicit operations by helping to move money around. Some are naive teenagers who work from home for part-time pay and may not know that they are part of an international fraud ring. Criminals who have stolen sensitive financial account information from a victim's PC using a trojan horse, spyware, or adware direct the mule to make a cash withdrawal from the financial account and then wire the stolen money to a bank account overseas.[50]

Insiders, such as in-house financial specialists, accountants, or bank employees in offshore zones or major financial centers, may also help cyber criminals evade the scrutiny of bank regulators and international investigators, deliberately or sometimes unwittingly.[51]

### *Law Enforcement Issues*

According to Secret Service Director Ralph Basham, "With just a few keystrokes, cyber criminals around the world can disrupt our economy."[52] However, according to some experts, statistics describing the extent of cyber crime are not reliable, partly because cyber crime is a vast area with innumerable crimes where no common statistics system exists. The Government Accountability Office (GAO) estimates that losses associated with cyber crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing. These projected losses are based on direct and indirect costs that may include actual money stolen, estimated cost of intellectual property stolen, and recovery cost of repairing or replacing damaged networks and equipment.[53]

In one example of costs associated with a computer security breach, TJX, the parent company of retailer TJ Maxx, took a $12 million charge in its fiscal first quarter of 2008 due to the theft, starting in 2006, of more than 45 million credit and debit card numbers. The costs were for investigating and containing the intrusion, improving computer security, communicating with customers, and other fees. TJX estimates that, adding damages from future lawsuits, the breach may eventually cost $100 per lost record, or a total of $4.5 billion.[54]

It is estimated that only 5 percent of cyber criminals are ever arrested or convicted, because the anonymity associated with Web activity makes them hard to catch and the trail of evidence needed to link them to a cyber crime is hard to follow. In response to numerous security breaches that can lead to credit card or checking account fraud, a number of states have enacted various identity theft laws to protect consumers. Many states now require notification by a business when there is evidence that consumer information may have been stolen by cyber criminals.[55] Fighting cyber crime requires cooperation between law enforcement and private industry, according to FBI Director Robert Mueller, who told a conference of computer security professionals in 2006 that "maintaining a code of silence" does not benefit a company in the long run. Steven Martinez, Deputy Assistant Director of the FBI's cyber division, pointed out that partnerships between law enforcement, the academic community, and the private sector are the key to reducing cyber crime.[56]

Each year, a survey of thousands of security practitioners from U.S. corporations, government agencies, financial institutions, and universities is conducted by the Computer Security Institute (CSI) with help from the computer intrusion team of the FBI's San Francisco office.[57] The CSI Computer Crime and Security Survey, published annually, is a widely used source of information about how often computer crime occurs and how expensive these crimes can be. Preliminary key findings from the 2007 CSI survey were that "the average annual loss reported more than doubled, from $168,000 in last year's report to

$350,424 in this year's survey. Reported losses have not been this high in the last five years. Financial fraud overtook virus attacks as the source of the greatest financial loss."[58] However, some observers question the statistical validity of the CSI survey methodology.[59]

The Computer Emergency Response Team Coordination Center (CERT– CC) at Carnegie Mellon University has for years collected information about computer security incidents occurring nationwide, and until 2004 also published summary information about the number and types of computer security incidents reported. However, as Internet cyber attacks rapidly became more sophisticated, the methodology used by CERT–CC for capturing and reporting intrusions could not keep up. In 2004, the CERT–CC Web site stated, "Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, beginning in 2004, we stopped publishing the number of incidents reported."[60]

With the uncertainties of survey results concerning the financial costs of computer crime and of reports about the number and types of computer security incidents, there may yet be no statistically valid way to understand the real scope and intensity of cyber crime. The growing evidence of botnets and of other automated attacks suggests that the percentage of undetected and unreported cyber crime may be going up.

### *Problems Tracing Cyber Crime*

Law enforcement officials concede that they face major obstacles in tracing the profits and finances of cyber criminals. Online payment services, such as PayPal and E-Gold, enable criminals to launder profits. Although some companies have been convicted and fined for distribution of spyware (which silently captures personal information from users' PCs), other adware and spyware purveyors can still make millions of dollars per year. Law enforcement officials argue that even legitimate technology companies are lax in enforcing standards to determine the veracity of online advertisers who may be distributing spyware. Many spyware companies are hard to subject to legal action because they typically also offer some legitimate services. The finances that back cyber crimes are so distributed that they are difficult for law enforcement to figure out.[61]

### *International Convention on Cyber Crime*

The ability of cyber criminals to ignore borders allows them to exploit obstacles to international law enforcement. Cyber crime is a major international challenge, and attitudes and laws about what amounts to a criminal act of computer wrongdoing vary from country to country. However, the Council of Europe, a consultative assembly of 43 countries based in Strasbourg, France, adopted the Convention on Cybercrime in 2001. Effective July 2004, it was the first international treaty to deal with breaches of law "over the Internet or other information networks." The convention requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.[62] (The convention is discussed further in chapter 21 in this volume, "Internet Governance.")

The Electronic Privacy Information Center, in a June 2004 letter to the U.S. Senate Foreign Relations Committee, objected on privacy grounds to U.S. ratification of the convention, arguing that it would "create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[63] However, a coalition of U.S. industry associations, including the Business Software Alliance, the Cyber Security Industry Alliance, the American Bankers Association, the Information Technology Association of America, InfraGard, Verisign, and several others, urged the Foreign Relations Committee to recommend ratification of the convention,[64] which the Senate did on August 3, 2006. The United States will comply with the convention based on existing

U.S. Federal law; no new implementing legislation was expected to be required. Legal analysts say that U.S. negotiators succeeded in scrapping most objectionable provisions, thereby ensuring that the convention tracks closely with existing U.S. laws.

The United States did not sign a complementary protocol that contained provisions to criminalize racist language on the Internet.[65] The Department of Justice has said that the protocol would be contrary to the guarantee of freedom of expression contained in the first amendment to the U.S. Constitution.

### *Organized Cyber Crime*

Some large cyber criminal groups are transnational networks; members reportedly operate from locations all over the world to hack into systems, steal credit card information, and sell identities.[66] Organized crime is also recruiting teenagers who apparently feel safer doing illegal activity online than in the streets. A useful source of information is the "Virtual Criminology Report" from McAfee, which draws on input from European high-technology crime units and the FBI.[67] It suggests that criminal outfits are targeting top students from leading academic institutions and helping them acquire more of the skills needed to commit high- tech crime on a massive scale. It also finds that cyber criminals are being drawn to social networking and community sites where they load fake profiles and pages with adware, spyware, and trojan horses. Some cyber criminals collate personal information found online to formulate virtual twin identities for fraudulent purposes; innocent users of these sites often expose such data, obviating the need for sophisticated attacks. Password proliferation for consumer and work devices means that simple guesswork often unlocks the door. Removable media devices like flash drives make it easier to steal inside information. At least 12 million computers around the world are now compromised for use in botnets and are used for phishing schemes, illegal spamming, the spread of pornography, and the theft of passwords and identities. Smartphones and multifunctional mobile devices are making portable computers ubiquitous; cyber criminals will increasingly mine them for valuable information. The increasing use of Bluetooth and voice over Internet protocol will also lead to a new generation of phone hacking.[68]

In the future, we may see new and different modes of criminal organizations evolve in cyberspace. Cyberspace frees individuals from many of the constraints that apply to activities in the physical world. Cyber crime requires less personal contact, less need for formal organization, and no need for control over a geographical territory. Therefore, some researchers predict, the hierarchical structures of organized crime groups may adapt, and online criminal activity may instead emphasize lateral relationships and networks.[69] Instead of assuming stable personnel configurations that can persist for years, online criminal organization may reflect a "swarming" model: individuals coalesce for a limited period of time in order to conduct a specific task, or set of tasks, and afterward go their separate ways. This can make the task of law enforcement much more difficult. If cyber criminals evolve into the "Mafia of the moment" or the "cartel of the day," police will lose the advantage of identifying a permanent group of participants who engage in a set of repeated activities.[70]

### *Terrorism and Cyber Crime*

The proportion of cyber crime that can be directly or indirectly attributed to terrorists is difficult to determine. Linkages between criminal and terror groups may allow terror networks to expand internationally by leveraging the computer resources, money laundering activities, and transit routes of criminals. The 2005 subway and bus bombings and the 2007 attempted car bombings in the United Kingdom also indicate that groups of terrorists are active within countries that have large communications networks and computerized infrastructures, along with a large, highly skilled information technology workforce. London police officials reportedly believe that terrorists obtained the high-quality explosives used for the 2005 bombings through criminals based in Eastern Europe.[71]

A recent British trial revealed a significant link between Islamic terrorist groups and cyber crime. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, pled guilty and were sentenced for using the Internet to incite murder. The men had used 110 different stolen credit cards at online Web stores to purchase items such as night vision goggles, tents, global positioning satellite devices, hundreds of prepaid cell phones, and more than 250 airline tickets to be used by terrorists. Another 72 stolen credit cards were used to register over 180 Internet domains at 95 different Web hosting companies. The group laundered money charged to more than 130 stolen credit cards through online gambling Web sites. Their fraudulent charges totaled more than $3.5 million from a database containing 37,000 stolen credit card numbers along with account holders' names and addresses, dates of birth, credit balances, and credit limits.[72]

Regions with major narcotics markets, such as Western Europe and North America, have optimal technology infrastructure and open commercial nodes that are increasingly used for transnational trafficking by both criminal and terrorist groups.[73] Officials of the U.S. Drug Enforcement Administration (DEA) reported in 2003 that 14 of the 36 groups found on the U.S. State Department's list of foreign terrorist organizations were also involved in drug trafficking. A 2002 report by the Library of Congress Federal Research Division described a "growing involvement of Islamic terrorist and extremist groups in drug trafficking," along with some evidence of cooperation between terrorist groups involving both drug trafficking and trafficking in arms.[74] Consequently, DEA officials argued, the war on drugs and the war on terrorism are and should be linked.[75]

State Department officials stated at a Senate hearing in March 2002 that terrorist groups may be using drug trafficking as a way to both gain financing and to weaken their enemies in the West by spreading addictive drugs.[76] The poppy crop in Afghanistan reportedly supplies resin to produce over 90 percent of the world's heroin, supporting a drug trade estimated at $3.1 billion, some of which goes to fund terrorist and insurgent groups in Afghanistan. Intelligence reports in 2007 stated that al Qaeda in Afghanistan had been restored to its pre–September 11, 2001, operation levels, and may be in a better position now to strike Western countries.[77]

Drug traffickers are reportedly among the heaviest users of encryption for Internet computer messaging and have the wherewithal to hire high-level computer specialists to help evade law enforcement, coordinate drug shipments, and launder money. Such technologies also enable terrorist organizations to transcend borders and operate internationally with less chance of detection. Many highly trained technical specialists are located in the countries of the former Soviet Union and the Indian subcontinent. Some technical specialists would not willingly work for criminal or terrorist organizations, but many may be misled or unaware of their employers' terrorist objectives, while some agree to provide assistance because well-paid legitimate employment is scarce in their region.[78]

### *Future Targets: Infrastructure Control Systems*

Evidence has not yet been published showing a widespread focus by cyber criminals on attacking the control systems that operate the U.S. civilian critical infrastructure. Disabling infrastructure controls for communications, electrical distribution, or other infrastructure systems is often described as a way terrorists might seek to amplify the effects of a simultaneous conventional terrorist attack involving explosives. (See the discussion of critical infrastructure protection in chapter 23 in this volume, "Cyberpower and Critical Information Protection: A Critical Assessment of Federal Efforts.")

Criminal extortion schemes in which attackers have exploited control system vulnerabilities for economic gain have already occurred. In January 2008, officials from the Central Intelligence Agency stated:

> We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands…We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States…We do not know who executed these attacks or why, but all involved intrusions through the Internet.[79]

In December 2006, malicious software for an automated control system vulnerability scanner reportedly was made available on the Internet; this software would enable individuals with relatively little experience in control systems to scan a critical system and identify its vulnerabilities quickly.

Many, if not most, automated control systems are connected to the Internet or to corporate administrative systems and are vulnerable to a cyber attack. Because many of these systems were not originally designed with security as a priority, it is often difficult to implement new security controls to reduce known security vulnerabilities.[80] On the basis that hackers and cyber criminals will always seek to take advantage of easy vulnerabilities, some analysts now predict that cyber criminals will exploit vulnerabilities in critical infrastructure control systems.[81] The Idaho National Laboratory, one of 10 multiprogram National Laboratories operated by the Department of Energy, has been tasked to study and report on technology risks associated with infrastructure control systems.[82]

Some experts argue that cyber terrorism does not suit the objectives of terrorists because it does not cause the horrific visible effects of blood, smoke, and fire that cause terror. However, botnets might be used strategically to amplify the effects of a conventional terrorist attack, such as one using bombs, or perhaps by delaying or diverting first responders from such an attack.

## *The urgency of Improving Cyber Security*

In recent years, many software vendors have taken major steps to improve the security of their commercial products and to distribute software patches rapidly to fix newly discovered problems. However, much is still needed to help improve the computer security policy and practices of businesses and home users of these products. Cyber criminals continue to search for new vulnerabilities, and there is still far too much opportunity for them to take advantage of weaknesses in networks and systems that persist, despite publicity warning about the increasing threat of cyber crime.

As early as 1991, the National Research Council published a report titled "Computers at Risk" and another in 1993, titled "Trust in Cyberspace." Both warned that computer networking would allow cyber attacks to affect more users and would increase the number of potential attackers. The National Infrastructure Advisory Council, now a part of the Department of Homeland Security (DHS), was created in 2001 to improve cooperation for cyber security between banking, manufacturing, and other businesses and local and state governments and law enforcement. In 2002, Congress passed the Federal Information Security Management Act (FISMA), which was intended to improve computer and network security for Federal Government agencies. FISMA required yearly audits in which agencies must report on their compliance with specified standards and rules to strengthen cyber security, set by Congress, the executive branch, and the National Institute for Standards and Technology (NIST). The Cybersecurity Research and Development Act of 2002 authorized appropriations for the National Science Foundation and NIST to improve information-sharing between the private sector and government, and to increase the number of information security professionals. The 2003 White House statement, "The National Strategy to Secure Cyberspace," warned that cyber attack tools are becoming more sophisticated and widely available and that future organized cyber attacks could severely disrupt the Nation's civilian critical infrastructure, cripple the economy, and adversely affect national security.

Other reports specifically describe security vulnerabilities of computers that operate the civilian critical infrastructure. Water supply, electrical distribution, communications, and other industry sectors are operated by computerized control systems that are vulnerable to cyber attack. Such an incident could be used as a threat to extort money, could be damaged by an attack like the 2007 DDOS cyber attack in Estonia, or could be used to amplify the effects of a simultaneous physical terrorist attack.

Most infrastructure control systems are privately owned, but because of the risk to national security, Homeland Security Presidential Directive 7 directed DHS to coordinate efforts to protect the cyber security for the Nation's critical infrastructure. In 2005, DHS issued the "Interim National Infrastructure Protection Plan" and the "National Plan for Research and Development in Support of Critical Infrastructure Protection," providing a framework for identifying, prioritizing, and protecting each infrastructure sector.

However, many observers point out that there is still no apparent sense of national urgency to close the gap between cyber security and the threat of cyber attack. For example, despite FISMA, security remains a low priority or is treated almost as an afterthought at some domestic Federal agencies.[83] In 2004, a GAO report stated that cyber security risks had actually increased for attacks against infrastructure control systems for water, electricity, communications, and other sectors.[84] However, a more recent GAO report stated that the private sector had made progress for improving computer security, although that progress varied by industry sector.[85] Even as corporations and individual users gradually become more cautious in their policies and actions, critical infrastructure control systems may become more attractive as targets for cyber crime.

Cyber crime is one of the risks of doing business, but many decisionmakers currently seem to view it as a low-probability threat. Perhaps the information dangers have not been presented compellingly enough, or perhaps future possibilities are discounted, partly because the future costs of current inaction will not be borne by current decisionmakers.

Nevertheless, IT vendors must somehow be persuaded to regard security as a product attribute that is coequal with performance and cost; to value cyber security research as much as they value research into high performance or cost-effective computing; and to incur present-day costs in order to obtain future protection.[86]

The low risk of detection and identification will continue to embolden cyber criminals and will encourage them to further expand the scope of cyber crime, along with its consequences. Cyber criminals will continue to use new technologies and select new priorities and objectives to guide their cyber attacks. Cyber crime may give even more support to extremist groups in the future. Vulnerabilities in critical infrastructure control systems could attract new criminal activity to extort money or meet terrorist demands.

Cyber criminals are likely to make profitable alliances involving trade in lucrative items such as counterfeit goods or pirated intellectual property. Future cyber criminal organizations may have no central geographic base and may function effectively solely through network technology, taking on new forms that may be more difficult for law enforcement organizations to counter.

Policy issues for reduction of cyber crime include seeking new ways for private industry and government to cooperate for reporting cyber crime and increasing cyber security; encouraging more international cooperation among law enforcement agencies to improve attribution of cyber crimes and for pursuing malicious actors across national borders; and developing more accurate methods for measuring the effects of cyber crime.

As cyber crime is recognized by government and industry officials as a growing threat to national security, each business and government agency must be held more accountable for protecting against cyber crime by following best practices to improve computer security in their organizations. This may be problematic as long as the reporting of computer security vulnerabilities is viewed as a threat to customers' or users' confidence. Thus, businesses and government may need to create new ways to anonymously report cyber intrusions, while still holding management accountable for cyber security. Education programs to change public attitudes about reporting cyber intrusions may also help. Ultimately, reducing the threat to national security from cyber crime depends on a strong commitment by government and the private sector to follow best management practices that help improve computer security.

Security experts generally believe that terrorist groups collectively will not, at least in the near future, have the technical skills required to launch an effective, widespread cyber attack. However, the events in Estonia in 2007 and the growing threat from cyber crime may soon alter that sense of safety. Extremists may take advantage of criminal botnets and begin to employ cyber attack as a weapon, perhaps against critical civilian infrastructure of Western nations.

Cyber crime is likely to increase in variety, scope, and consequences until both government and industry decisionmakers make cyber security research and measurement a high priority, increase international coordination between governments and with business for reporting and investigating cyber attacks, and devote more resources to best practices to reduce computer security vulnerabilities.

[1] See also chapter 19 in this volume, "Cyber Terrorism: Menace or Myth?"

[2] Bruce Schneier, "Attack Trends: 2004 and 2005," *Schneier on Security* blog, June 6, 2005, available at <www.schneier.com/blog/archives/2005/06/attack_trends_2.html>.

[3] The Computer Crime and Intellectual Property Section of the U.S. Department of Justice is responsible for implementing national strategies in combating computer and intellectual property crimes worldwide. U.S.

Department of Justice Cybercrime Web site, available at <www.cybercrime.gov/>.

[4] "Turk, Moroccan nabbed in huge worm case," *CNNMoney.com*, August 26, 2005, available at <http://money.cnn.com/2005/08/26/technology/worm_arrest/index.htm>; Allen Wastler, "Virus angst, thy name is us," *CNNMoney.com*, August 25, 2005, available at <http://money.cnn.com/2005/08/17/commentary/wastler/wastler/index.htm>.

[5] Reuters, "Cybercrime is Getting Organized," *Wired*, September 15, 2006, available at <www.wired.com/techbiz/media/news/2006/09/71793>.

[6] Robert Vamosi, "Cyberattack in Estonia—What It Really Means," *CnetNews.com*, May 29, 2007, available at <http://news.com.com/Cyberattack+in+Estonia-what+it+really+means/2008-7349_3-6186751.html>.

[7] Iain Thomson, "Russia 'Hired Botnets' for Estonia cyber-war," *VnuNet.com*, May 31, 2007, available at <www.vnunet.com/vnunet/news/2191082/claims-russia-hired-botnets>.

[8] Heise Security, "Estonian DDoS—A Final Analysis," May 31, 2007, available at <www.heise-security.co.uk/news/print/90461>.

[9] "Cyber attack Fallout in Estonia," February 4, 2008, *The Budapest Times*, February 4, 2008, available at <www.budapesttimes.hu/index.php?option=com_content&task=view&id= 5081&Itemid=26>.

[10] Examples are Defcon (<www.defcon.org/>) and the Blackhat Security Conference (<www.blackhat.com/>), both held annually.

[11] "McAfee Virtual Criminology Report: Organized Crime and the Internet," December 2006, available at <www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_ Criminology_Report_2006.pdf>.

[12] A Web crawler (also known as a Web spider or Web robot) is a program or automated script that browses the World Wide Web systematically. Web crawlers are mainly used to create a copy of all the visited pages for later processing by a search engine that will index the downloaded pages to provide fast searches. "Web Crawler," *Wikipedia*, available at <http://en.wikipedia.org/wiki/Web_crawler>.

[13] Gregory Crabb, U.S. Postal Service Global Investigations, and Yuval Ben-Itzhak, CTO Finjan, presentation at the Gartner IT Security Summit 2007, Washington, DC, June 4, 2007.

[14] Trojan horses, spyware, and adware are forms of malicious software that can secretly infect a computer, record sensitive information residing on that computer, or log keystrokes (including passwords), and then transmit that information through the Internet to a temporary location where it is collected for fraudulent use by a third party.

[15] Bob Keefe, "PC Security Still More of a Wish than a Promise," *Atlanta Journal*, February 3, 2007, 1A; U.S. Department of Justice for the Central District of California, "'Botherder' Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code," Release 06–051, May 8, 2006, available at <www.usdoj.gov/criminal/cybercrime/ anchetaSent.htm>.

[16] Julie Bort, "Attack of the Killer Bots," *Network World*, July 2/9, 2007, 29.

[17] Susan MacLean, "Report Warns of Organized Cyber Crime," *ItWorldCanada*, August 26, 2005, available at <www.itworldcanada.com/a/IT-Focus/39c78aa4-df47-4231-a083-ddd1ab8985fb.html>.

[18] "McAfee Virtual Criminology Report: Organized Crime and the Internet."

[19] Elise Ackerman, "Hackers' Infections Slither Onto Web Sites," *Mercury News*, January 3, 2007, 1.

[20] Jeff Hecht, "Web Browsers Are New Frontline in Internet War," *NewScientistTech*, May 5, 2007, available at <www.newscientisttech.com/article.ns?id=mg19426026.000&print=true>; Niels Provos et al., "The Ghost in the Browser: Analysis of Web-based Malware," available at <www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf>.

[21] Finjan, Inc., "Web Security Trends Report, Q2 2007," June 2007, available at <www.finjan.com/Content.aspx?id=827>.

[22] Lou Bobson, "Identity Theft Ruining Lives," *The Sunday Mail*, May 20, 2007, 62.

[23] "A Chronology of Data Breaches," Privacy Rights Clearinghouse, available at <www.privacyrights.org/ar/ChronDataBreaches.htm#CP>. See also David Bank and Christopher Conkey, "New Safeguards for Your Privacy: Bank Regulators are Latest to Push for Alerts to Consumers When Personal Data Get Breached," *The Wall Street Journal*, March24, 2005, D1, available at <http://online.wsj.com/article/SB111162452521088223.html>.

[24] Dawn Onley and Patience Wait, "DOD's Efforts to Stave Off Nation-state Cyberattacks Begin with China," *Government Computer News*, August 21, 2006.

[25] Computer Crime Research Center, "Russia, Biggest Ever Credit Card Scam," July 8, 2005, available at <www.crime-research.org/news/08.07.2005/1349/>.

[26] David Hayes, "A Dollar Goes a Long Way in Swiping Private Data," *Kansas City Star*, March 20, 2007, 1.

[27] "European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) 2001/2098(INI)," approved on September 5, 2001, available at <www.cyber-rights.org/ interception/echelon/European_parliament_resolution.htm>; Ron Pemstein, "Europe Spy System," GlobalSecurity.org, March 30, 2000, available at <www.globalsecurity.org/intell/library/news/2000/03/000330-echelon1.htm>; Gerhard Schmid, "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)," Document A5-0264/2001, May 9, 2001, available at <www.statewatch.org/news/2001/sep/02echelon.htm>.

[28] James Woolsey, "Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage," Federation of American Scientists, March 7, 2000, available at <http://ftp.fas.org/irp/news/2000/03/wool0300.htm>.

[29] James Lewis, testimony before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, April 15, 2007.

[30] Chris Johnson, "Naval War College Network, Web Site Back Up Following Intrusion," *Inside the Navy*, December 18, 2006.

[31] Robert McMillan, "Pentagon Shuts Down Systems After Cyber-Attack," *PC World*, June 21, 2007, available at <www.pcworld.com/article/id,133301-pg,1/article.html>.

[32] In addition, some estimates say that up to 90 percent of computer software used in China is pirated and thus open to hijack through computer viruses. James Lewis, "Computer Espionage, Titan Rain and China," Center for Strategic and International Studies, December 14, 2005.

[33] Josh Rogin, "Cyber Officials: Chinese Hackers Attack 'Anything and Everything'," *FCW.com*, February 13, 2007, available at <www.fcw.com/article97658-02-13-07-Web&printLayout>.

[34] The Global Business Security Index reports worldwide trends in computer security from incidents that are collected and analyzed by IBM and other security organizations. IBM press release, "IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005," August 2, 2005.

[35] "McAfee Virtual Criminology Report: Organized Crime and the Internet."

[36] Marisa Randazzo et al., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," Carnegie Mellon Software Engineering Institute, August 2004, available at <www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr021.pdf>.

[37] U.S. Attorney's Office, District of Connecticut, Antiterrorism Advisory Council, available at <www.usdoj.gov/usao/ct/attf.html>.

[38] Jaroslaw Anders, "Copyright Violations Threaten Cultural Diversity," U.S. Department of State, April 26, 2007, available at <http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2007&m=April&x=20070426164247zjsredna0.739773>.

[39] Frederick Balfour et al., "Fakes!" *Business Week*, February 7, 2005, 54–64.

[40] "MEPs back criminal sanctions for counterfeiters," *EurActiv.com*, April 25, 2007, available at <www.euractiv.com/en/innovation/meps-back-criminal-sanctions-counterfeiters/ article-163380>.

[41] Nancy Gohring, "Feds Renew Cybercrime Fight," *PC World*, June 28, 2007, available at <www.pcworld.com/article/id,133523-c,cybercrime/article.html>.

[42] U.S. Department of Justice Press Release, "Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting," April 27, 2007, available at <www.usdoj.gov/opa/pr/2007/April/07_crm_301.html>.

[43] "ShadowCrew was an international crime message board that offered a haven for carders or 'hackers' to trade, buy, and sell anything from stolen personal information, to hacked credit card numbers and false identification. ShadowCrew emerged from another underground site, counterfeitlibrary.com in early 2002 and would be followed up by carderplanet.com, a primarily Russian site…The site flourished from the time it opened in 2002 until its demise in late October 2004." "ShadowCrew," *Wikipedia*, available at <http://en.wikipedia.org/wiki/ShadowCrew>.

[44] Brian Grow et al., "Gold Rush," *Business Week*, January 9, 2006, 68–76.

[45] Ibid.

[46] Council of Europe Octopus Programme, *Summary of the Organised Crime Situation Re- port 2004: Focus on the Threat of Cybercrime* (Strasbourg: Council of Europe, September 6, 2004), 47.

[47] Catherine Holahan, "Policing Online Money Laundering," *Business Week Online*, November 6, 2006, 4, available at <www.businessweek.com/technology/content/nov2006/tc20061106_986949.htm?campaign_id=bier_tcv.g3a.rssf1106u>.

[48] "Neteller, the market-leading 'virtual wallet' payment processor, closed down its American operations after the arrest this week of its two Canadian founders…Over six months last year, Neteller processed transactions worth $5.1bn (£2.6bn), with about 85% involving American customers." "Arrests prompt Neteller to quit U.S. gaming," *Guardian Unlimited*, January 19, 2007, available at <www.guardian.co.uk/technology/2007/jan/19/news.newmedia>; Reuters, "Company Reaches Deal with U.S. in Internet in Internet Gambling Case," *The New York Times*, July 19, 2007, available at <www.nytimes.com/2007/07/19/business/worldbusiness/19neteller.html>.

[49] "PayPal Express Looks for More Pals as it Battles Google Checkout," *Internet Retailer*, May 18, 2007, available at <www.internetretailer.com/dailyNews.asp?id=22446>. It was reported that "61% of [PayPal's] payment volume came from eBay.com, the auction site that owns PayPal." See also Holahan, 4.

[50] Ken Dunham, "Money Mules: An Investigative View," *Information Systems Security* (March- April 2006), 6.

[51] Louise I. Shelley and John T. Picarelli, "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism," *Police Practice and Research* 3, no. 4 (2002), 311, available at <www.american.edu/traccc/Publications/ Shelley%20Pubs/To%20Add/MethodsnotMotives.pdf>.

[52] Marcia Savage, "Private-public Sector Rallies Against Organized Cybercrime," *SCMagazine. com*, February 17, 2005, available at <www.scmagazineus.com/Private-public-sector-rallies-against-organized-cybercrime/article/31800/>.

[53] U.S. Government Accountability Office, "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," Report GAO–07–705, June 2007, available at <www.gao.gov/new.items/d07705.pdf>.

[54] Sharon Gaudin, "Breach Costs Soar at TJX," *Information Week*, May 21, 2007, 19.

[55] "State PIRG Summary of State Security Freeze and Security Breach Notification Laws," available at <www.pirg.org/consumer/credit/statelaws.htm>.

[56] Marcia Savage, "Companies Still Not Reporting Attacks, FBI Director Says," *SearchSecurity.com*, February 15, 2006, available at <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1166845,00.html>.

[57] "Virus Attacks Named Leading Culprit of Financial Loss by U.S. Companies in 2006 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, July 13, 2006, available at <www.gocsi.com/press/20060712.jhtml>.

[58] Robert Richardson, "CSI Computer Crime and Security Survey 2007," available at <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>.

[59] The survey is limited to CSI members, and thus respondents may not be representative of all security practitioners, and their employers may not be representative of employers in general. In addition, as the 2006 CSI/FBI survey itself points out, most companies are continuing to sweep security incidents under the rug. Bill Brenner, "Security Blog Log: Has CSI/FBI Survey Jumped the Shark?" *SearchSecurity.com*, July 21, 2006, available at <http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1202328,00.html>.

[60] CERT Coordination Center, Carnegie Mellon University, 2004, accessed at <www.cert.org/stats/>.

[61] Matt Hines, "Malware Money Tough to Trace," *Eweek*, September 18, 2006, 14.

[62] Full text of the Convention on Cybercrime is available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[63] Marc Rotenberg, Cedric Laurant, and Tara Wheatland, letter to Richard G. Lugar and Joseph R. Biden, Jr., June 17, 2004, available at <www.epic.org/privacy/intl/senateletter-061704.pdf>.

[64] Patience Wait, "Industry Groups Urge Senate Ratification of Cybercrime Treaty," *Government Computer News*, June 6, 2005, available at <http://appserv.gcn.com/vol1_no1/web/36257-1.html>; Declan McCullagh, "Tech Firms Call for Approval of Cybercrime Treaty," *CNet News.com*, June 29, 2005, available at <http://news.com.com/2102-7348_3-5768462.html?tag=st.util.print>.

[65] The U.S. Senate Committee on Foreign Relations held a hearing on the convention on June 17, 2004. Kristin Archick, "Cybercrime: The Council of Europe Convention," Congressional Research Service Report RS21208, April 26, 2002, available at <http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-2394:1>; Estelle Durnout, "Council of Europe Ratifies Cybercrime Treaty," *ZDNet*, March 22, 2004, available at <http://news.zdnet.co.uk/business/legal/0,39020651,39149470,00.htm>.

[66] Kevin Poulsen, "Feds Square Off with Organized Cyber Crime," *SecurityFocus*, February 17, 2005, available at

<www.securityfocus.com/news/10525>.

[67] McAfee Virtual Criminology Report, “Cybercrime: The Next Wave,” 2007, available at <www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_en.pdf>.

[68] Bill Brenner, “Criminals Find Safety in Cyberspace,” *SearchSecurity.com*, December 18, 2006, available at <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1235455,00.html?bucket=NEWS&topic=299990>.

[69] “Summary of the Organised Crime Situation Report 2004: Focus on the Threat of Cybercrime,” 48.

[70] Susan Brenner, “Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships,” *North Carolina Journal of Law and Technology* 4, no. 1 (Fall 2002), available at <www.jolt.unc.edu/Vol4_I1/Web/Brenner-V4I1.htm>.

[71] Conal Walsh, “Terrorism on the Cheap—and with No Paper Trail,” *The Guardian*, July 17, 2005, available at <www.guardian.co.uk/business/2005/jul/17/alqaida.money>; Rollie Lal, “Terrorists and Organized Crime Join Forces,” *International Herald Tribune*, May 25, 2005, available at <www.iht.com/articles/2005/05/23/opinion/edlal.php>; Barbara Porter, “Forum Links Organized Crime and Terrorism,” *By George!*, Summer 2004, available at <www2.gwu.edu/~bygeorge/060804/crimeterrorism.html>.

[72] Brian Krebs, “Three Worked the Web to Help Terrorists,” *The Washington Post*, July 6, 2007, D1.

[73] Glenn Curtis and Tara Karacan, “The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe,” Federal Research Division, Library of Congress, December 2002, 22, available at <www.loc.gov/ rr/frd/pdf-files/WestEurope_NEXUS.pdf>.

[74] LaVerle Berry, Glenn E. Curtis, Rex A. Hudson, and Nina A. Kollars, “A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups,” Federal Research Division, Library of Congress, May 2002, available at <www.loc.gov/rr/frd/ pdf-files/NarcsFundedTerrsExtrems.pdf>.

[75] Authorization for coordinating the Federal war on drugs expired on September 30, 2003. For more information, see Mark Eddy, “War on Drugs: Reauthorization of the Office of National Drug Control Policy,” CRS Report RL32352 (Washington, DC: Congressional Research Service, June 1, 2005), available at <www.fas.org/sgp/crs/misc/RL32352. pdf>. Also see D.C. Préfontaine and Yvon Dandurand, “Terrorism and Organized Crime: Reflections on an Illusive Link and its Implication for Criminal Law Reform,” International Society for Criminal Law Reform Annual Meeting, Montreal, August 8–12, 2004, available at <www.icclr.law.ubc.ca/Publications/Reports/International%20Society%20Paper%20of%20Terrorism.pdf>.

[76] Rand Beers and Francis X. Taylor, U.S. State Department, “Narco-Terror: The Worldwide Connection Between Drugs and Terror,” testimony before the U.S. Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, March 13, 2002, available at <www.state.gov/p/inl/rls/rm/8743.htm>.

[77] Matthew Lee and Katherine Shrader, “Al-Qaeda Has Rebuilt, U.S. Intel Warns,” *Associated Press*, July 12, 2007, available at <http://news.yahoo.com/s/ap/20070712/ap_on_go_pr_wh/us_terror_threat_32;_ylt=AuURr2eP8AhBrfHyTOdw714Gw_IE>; Associated Press, “Afghanistan’s poppy crop could yield more than 2006’s record haul, UN says,” *International Herald Tribune*, June 25, 2007, available at <www.iht.com/articles/ ap/2007/06/25/asia/AS-GEN-Afghan-Drugs.php>.

[78] Louise Shelly, “Organized Crime, Cybercrime, and Terrorism,” Computer Crime Research Center, September 27, 2004, available at <www.crime-research.org/articles/Terrorism_Cybercrime/>.

[79] “CIA Confirms Cyber Attack Caused Multi-City Power Outage,” *SANS NewsBites* X, no. 5, January 18, 2008, available at <www.sans.org/newsletters/newsbites/newsbites. php?vol=10&issue=5>.

[80] Aaron Turner, testimony to House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, hearing on “Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure,” April 19, 2007, available at <http://homeland.house.gov/SiteDocuments/20070419153130-95132.pdf>.

[81] Ibid.

[82] Idaho National Laboratory, “National Security: Energy Security,” available at <www.inl.gov/nationalsecurity/energysecurity/>.

[83] James A. Lewis, statement to Committee on House Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement, Subcommittee on Information Policy, Census, and National Archives, June 7, 2007.

[84] U.S. General Accounting Office, “Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,” GAO–04–354, March 2004, available at <www.gao.gov/new.items/d04354.pdf>.

[85] U.S. Government Accountability Office, "Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics," GAO–07–39, October 16, 2006, available at <www.gao.gov/new.items/d0739.pdf>.

[86] Seymour Goodman and Herbert Lin, eds., *Toward a Safer and More Secure Cyberspace* (Washington, DC: Committee on Improving Cybersecurity Research in the United States, National Research Council, 2007), 261–267, available at <http://books.nap.edu/openbook.php?isbn=0309103959>.