business. A military organization may find its communications disrupted. A government or nonprofit organization may be unable to get its message out to the public.

A DoS attack is an example of an "asymmetric" attack, in which a single person can harm a huge organization, such as a multinational corporation or even a government. Since terrorist organizations specialize in asymmetric attacks, some fear that DoS attacks will become an important part of the terrorist arsenal [42, 43].

In a **distributed** denial-of-service (DDoS) attack, the attacker rents access to a botnet from a **bot herder**. At the selected time, the command-and-control computer sends the appropriate instructions to the bots, which launch their attack on the targeted system.

7.4.2 Cyber Crime

Criminal organizations have discovered that a great deal of money can be made from malware, so many of them have entered the arena, raising the stakes for corporations and individuals trying to protect their systems and sensitive information, respectively. Edward Skoudis paints a grim picture of the contemporary landscape:

> Some attackers sell to the highest bidder customized malicious code to control victim machines. They may rent out armies of infected systems useful for spam delivery, phishing schemes, denial-of-service attacks, or identity theft. Spyware companies and overly aggressive advertisers buy such code to infiltrate and control victim machines. A single infected machine displaying pop-up ads, customizing search engine results, and intercepting keystrokes for financial accounts could net an attack $1 per month or more. A keystroke logger on an infected machine could help the attacker gather credit card numbers and make $1,000 or more from that victim before the fraud is discovered. With control of 10,000 machines, an attacker could set up a solid profit flow from cyber crime. Organized crime groups may assemble collectives of such attackers to create a business, giving rise to a malicious code industry. In the late 1990s, most malicious code publicly released was the work of determined hobbyists, but today, attackers have monetized their malicious code; their profit centers throw off funds that can be channeled into research and development to create more powerful malicious software and refined business models, as well as to fund other crimes. [40]

In this section, we review a few well-known cyber crime incidents.

JEANSON JAMES ANCHETA

In 2004 and 2005, Internet cafe employee Jeanson James Ancheta created a network of about 400,000 bots, including computers operated by the U.S. Department of Defense. Adware companies, spammers, and others paid Ancheta for the use of these computers. After being arrested by the FBI, Ancheta pleaded guilty to a variety of charges, including conspiring to violate the Computer Fraud Abuse Act and the CAN-SPAM Act. In May 2005, a federal judge sentenced Ancheta to 57 months in prison and required him to pay $15,000 in restitution to the U.S. government for infecting Department of Defense computers. Ancheta also forfeited to the government the proceeds of his illegal activity, including his 1993 BMW, more than $60,000 in cash, and his computer equipment [44, 45].

PHARMAMASTER

Israeli company Blue Security created a spam-deterrence system for people tired of receiving unwanted email. Blue Security sold the service to businesses, but individuals could protect their home computers for free. About half a milion people signed up for this free service. Users loaded a bot called Blue Frog on their computers. The bot integrated with Yahoo! Mail, Gmail, and Hotmail, checking incoming email messages for spam. When it discovered a spam message, the bot would contact a Blue Security server to determine the source of the email. Then the bot would send the spammer an opt-out message [46].

Spammers who indiscriminately sent emails to millions of addresses started receiving hundreds of thousands of opt-out messages, disrupting their operations. Six of the world's top ten spammers agreed to use Blue Security's filtering software to remove Blue Frog users from their email lists [46].

One spammer, nicknamed PharmaMaster, did not back down. He threatened Blue Frog users with messages such as this one: "Unfortunately, due to the tactics used by Blue Security, you will end up receiving this message or other nonsensical spams 20–40 times more than you would normally" [37]. He followed through on his threats on May 1, 2006, by sending Blue Frog users 10 to 20 times as much spam as they would normally receive [46].

The next day, PharmaMaster went after Blue Security itself. He launched a massive DDoS attack from tens of thousands of bots targeting Blue Security's servers. The huge torrent of incoming messages disabled the Blue Frog service. Later DDoS attacks focused on other companies providing Internet services to Blue Security. Finally, the spammer targeted the businesses that paid for Blue Security's services. When Blue Security realized it could not protect its business customers from DDoS attacks and virus-laced emails, it reluctantly discontinued its service. "We cannot take the responsibility for an ever-escalating cyberwar through our continued operations," wrote Eran Reshef, CEO of Blue Security. "We are discontinuing all of our anti-spam activities" [46]. Blue Security's decision to fight bots with bots—always controversial—was ultimately unsuccessful.

ALBERT GONZALEZ

In 2010, Albert Gonzalez was sentenced to 20 years of imprisonment after pleading guilty to using an SQL injection attack to steal more than 130 million credit and debit card numbers. Some of the credit and debit card numbers were sold online, leading to unauthorized purchases and bank withdrawals. The targets of the attacks were Heartland Payment Systems, 7-Eleven, Hannaford Brothers Supermarkets, TJX, DSW, Barnes and Noble, Office Max, and the Dave & Buster's chain of restaurants. Most of the numbers were stolen from Heartland Payment Systems, which estimated its losses at $130 million [47, 48].

AVALANCHE GANG

The Avalanche Gang is the name given the criminal enterprise responsible for more phishing attacks than any other organization. The Anti-Phishing Working Group (APWG) estimated that the Avalanche Gang was responsible for two-thirds of all global phishing attacks launched in the second half of 2009. In the second half of 2010, APWG noticed that Avalanche had nearly ceased its phishing attacks, leading to APWG to speculate that Avalanche was changing strategies and focusing on the propagation of spam that tricks people into downloading the Zeus Trojan Horse [49].

7.4.3 Politically Motivated Cyber Attacks

A cyber attack is a "computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it" [50]. Some nation states, terrorist organizations, and allied groups are mounting politically motivated cyber attacks on the computer and network infrastructure of their opponents, and some of these efforts have caused major disruptions.

ESTONIA (2007)

The small Baltic country of Estonia was part of the Soviet Union from the end of the Second World War until it became independent in 1991, and ethnic Russians still make up about a quarter of its population. In the capital city of Tallinn, a large bronze statue of a Soviet soldier had long been point of controversy between Estonians and Russians. Russians saw it as a symbol of the sacrifices made by Soviet troops in the victory over Germany in the Great Patriotic War, while Estonians saw it as a symbol of the oppressive Soviet occupation.

After 16 years of independence, the Estonian government decided to relocate the controversial statue from downtown Tallinn to a Russian military cemetery in the suburbs. They knew the relocation would be hugely unpopular with the Russians. In fact, the Russian government had warned that removing the statue would be "disastrous for Estonians" [51]. The police were prepared for violence, and although ethnic Russians rioted for two nights after the statue was moved, the damage was limited.

The government also expected an attack on its cyber infrastructure. Sure enough, an attack came, but its magnitude was greater than anything expected by the government's Internet security group. DDoS attacks from nearly a million computers targeted Estonian government ministries and all of Estonia's major commercial banks, telecommunications companies, and media outlets. To combat the attacks, much of Estonia's Internet was made inaccessible to computers outside the country, and on May 10, Estonia's largest bank had to suspend online services for an hour [51, 52].

In 2009, a group of Russian activists connected with Nashi, a pro-Kremlin youth group, claimed responsibility for the cyber attacks [53].

GEORGIA (2008)

Georgia is another former Soviet republic that gained independence in 1991. South Ossetia, a region of Georgia adjacent to Russia, gained de facto autonomy from Georgia after a brief war in 1991, though it continues to be recognized as a part of Georgia by the international community. On August 7, 2008, after provocations by South Ossetian separatists, Georgia sent troops into South Ossetia. Russian forces entered South Ossetia on August 8, and Russian and Georgian troops fought in South Ossetia for four days. A ceasefire between Georgia and Russia was signed a week later.

The conflict between Georgia and Russia is notable because even before Russian troops had entered South Ossetia, the Georgian government suffered a series of DDoS attacks that affected its ability to communicate with the outside world. Multiple Web sites went down for hours. The Georgian government went so far as to switch some of its Web hosting locations to the United States. American security experts said they had uncovered evidence of involvement by the Russian Business Network, a criminal gang located in St. Peterburg, but there was no clear link to the Russian military [54, 55, 56].

GEORGIA (2009)

Twitter service was unavailable *worldwide* for several hours on August 6, 2009, due to a massive DDoS attack. Max Kelly, the chief security officer at Facebook, said the attack was an effort to silence a political blogger from the Republic of Georgia, citing as evidence the fact that three other sites used by the activist—Facebook, LiveJournal, and Google—were also targets of DDoS attacks at the same time [57, 58].

No group took responsibility for the attacks, but some noted that August 6, 2009, was the first anniversary of the war between Georgia and Russia over South Ossetia [59].

EXILED TIBETAN GOVERNMENT (2009)

In 2009, computer security experts uncovered a surveillance effort targeting the Dalai Lama, the exiled Tibetan government, and other Tibetans. Some agency had used backdoor Trojans to penetrate 1,295 computers in 103 countries, creating a spying system the experts named GhostNet. When a victim opened an email attachment supposedly containing the translation of a book, the backdoor Trojan was activated. Each backdoor Trojan was able to transfer data files and email messages back to the controlling computer. Even more ominously, it could access the computer's microphone, turning the PC into an eavesdropping station. Some of the researchers that discovered GhostNet blamed the Chinese government for the intrusions, but the Chinese government denied responsibility [60, 61].

UNITED STATES AND SOUTH KOREA (2009)

A DDoS attack on governmental agencies and commercial Web sites in the United States and South Korea paralyzed a third of them over the Fourth of July weekend in 2009. Targets in the United States included the White House, the Treasury Department, the Secret Service, the New York Stock Exchange, and Nasdaq. In South Korea, the targets included the Blue House (presidential mansion), the Defense Ministry, and the National Assembly.

The DDoS attack was relatively minor, involving a botnet containing only 50,000–65,000 computers, compared with large-scale attacks that may utilize a million computers. Still, the attack disrupted different networks over a period of days as it shifted targets, and some sites in South Korea were unavailable or compromised as late as July 9. South Korea's National Intelligence Service blamed the North Korean government or its sympathizers for the attack, hypothesizing that the attack was in retaliation for United Nations sanctions against North Korea. According to computer experts, it was unlikely the source of the attack would ever be positively identified because those responsible for the attack launched it from systems owned by others [62, 63].

STUXNET WORM (2009)

Industrial processes such as chemical plants, oil and gas pipelines, and electrical power grids require constant monitoring. In the pre-computer era, monitoring was done by employees who watched gauges and warning lights, turned dials, and opened and closed valves. Computers allowed the automation of centralization of monitoring. In the 1980s, distributed control systems eliminated local control cabinets. Instead, networks carried information to centralized control centers. Computer monitors with color-coded fields replaced the gauges and warning lights. Initially, distributed control systems were proprietary, but customers asked for "open systems, common protocols and vendor interoperability" [64]. They got what they wanted with the advent of Supervisory Control and Data Acquisition (SCADA) systems based on the Internet Protocol. Internet-based SCADA systems are less expensive and are easier to maintain and administer than proprietary systems (Figure 7.5). Another way to save money and time is to allow an outsider to connect with the SCADA system remotely to perform diagnostics.

These advances carry with them security risks. Allowing remote diagnostics creates an opportunity for a malicious outsider to gain access. Many industrial machines

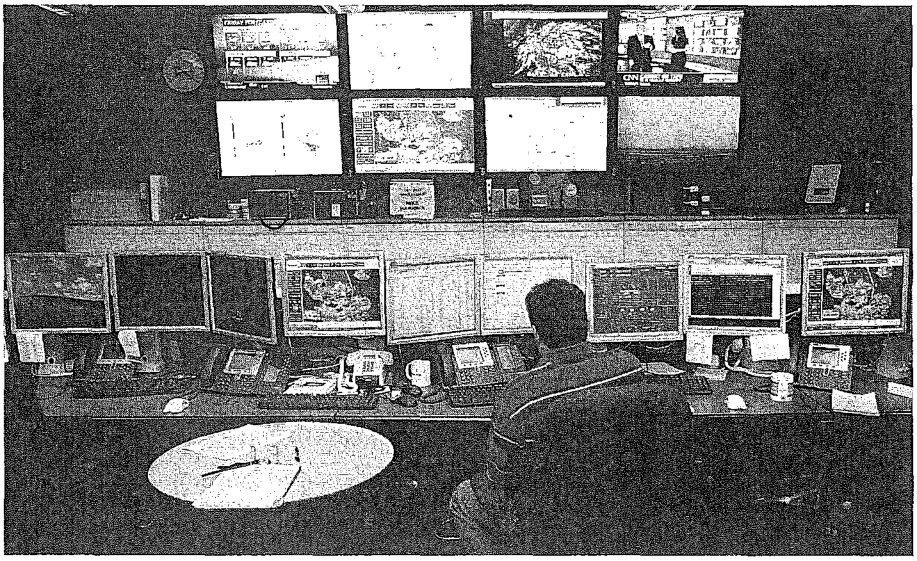

Figure 7.5 Internet-based supervisory control and data acquisition systems can save money and make systems easier to administer, but they also carry security risks. (© p77/ZUMA Press/Newscom)

contain embedded microprocessors. Industrial machines last a long time, which means many of these machines contain older microprocessors. Security patches designed to ward off malware may not be available for these microprocessors, and even if they are available, it may be impractical to install them because the processor is so slow that it cannot run the security code and keep up with its machine-control responsibilities.

The Stuxnet worm, launched in 2009, attacked SCADA systems running Siemens software [65]. The worm appeared to target five industrial facilities in Iran, and it may have caused a temporary shutdown of Iran's nuclear program by infecting computers controlling centrifuges processing uranium [66, 67]. There is some evidence that Israeli Defense Forces may have been responsible for unleashing the worm [68].

7.5 Online Voting

Throughout this chapter, we have seen many ways in which malefactors can breech the security of networked computers, yet the convenience and low cost of completing many tasks online are significant benefits. It should come as no surprise, then, that an online solution is often proposed when there is a problem with a traditional process. In this section, we evaluate a proposal to conduct elections over the Internet.

7.5.1 Motivation for Online Voting

The 2000 Presidential election was one of the closest contests in U.S. history. Florida was the pivotal state; without Florida's electoral votes, neither Democrat Al Gore nor Republican George W. Bush had a majority of votes in the Electoral College. After a manual recount of the votes in four heavily Democratic counties, the Florida Secretary of State declared that Bush had received 2,912,790 votes to Gore's total of 2,912,253. Bush's margin of victory was incredibly small: less than 2 votes out of every 10,000 votes cast.

Most of these counties used a keypunch voting machine in which voters select a candidate by using a stylus to poke out a hole in a card next to the candidate's name. Two voting irregularities were traced to the use of these machines. The first irregularity was that sometimes the stylus doesn't punch the hole cleanly, leaving a tiny, rectangular piece of card hanging by one or more corners. Votes with "hanging chad" are typically not counted by automatic vote tabulators. The manual recount focused on identifying ballots with hanging chad that ought to have been counted. The second irregularity was that some voters in Palm Beach County were confused by its "butterfly ballot" and mistakenly punched the hole corresponding to Reform Party candidate Pat Buchanan rather than the hole for Democratic candidate Al Gore (Figure 7.6). This confusion may have cost Al Gore the votes he needed to win Florida [69].

7.5.2 Proposals

The problems with the election in Florida led to a variety of actions to improve the reliability of voting systems in the United States. Many states replaced paper-based systems