Excerpts from:

Information Warfare and Security

Dorothy E. Denning
Georgetown University

acm PRESS
ADDISON WESLEY
ACM PRESS BOOKS

ADDISON-WESLEY

An imprint of Addison Wesley Longman, Inc.
Reading, Massachusetts • Harlow, England • Menlo Park, California
Berkeley, California • Don Mills, Ontario • Sydney
Bonn • Amsterdam • Tokyo • Mexico City

Chapter 3

Playgrounds to Battlegrounds

Information warfare is not an isolated activity; it is situated in the context of human action and human conflict. This chapter summarizes activity in four domains: play, crime, individual rights, and national security. The domain of play covers computer hacking, particularly system break- ins and acts committed mostly for fun. It involves conflicts between the hackers and the owners of the systems they penetrate and exploit. The domain of crime covers illegal acts, including intellectual property crimes and computer fraud and abuse. It involves conflicts between the perpetrators and victims of crimes. The domain of individual rights covers conflicts over free speech and privacy. These arise between individuals and between individuals and organizations or governments. Finally, the domain of national security addresses conflicts at a national level. It includes foreign intelligence operations, war and military conflict, terrorism, and operations against a nation by nonstate players.

The domains are not entirely disjoint. Hacking is usually a crime and often violates privacy. It is more than child's play and may be employed by organized crime groups, government intelligence agencies, military units, or terrorist organizations. Criminal acts that threaten the economy of a nation have national security implications. Acts that infringe privacy or assert free speech may be crimes. Terrorist acts are also crimes. Further, the domains are not exhaustive, and some acts, for example, competitive intelligence operations, do not fall neatly into them.

From a defensive information warfare perspective, it can be difficult to know in which domain a particular attack arises. If computer systems are penetrated, is it a kid fooling around? An organized crime ring looking for credit card numbers to steal? A competitor or foreign government seeking trade or national secrets? A terrorist group trying to disrupt critical infrastructures? Fortunately, many defenses work across a spectrum of threats, so it is not always necessary to distinguish them in order to safeguard information resources.

This chapter outlines some of the activity in each domain. The methods themselves, along with case studies, are treated in greater depth in later chapters.

PLAY

In 1878-long before the invention of digital computers-AT&T hired teenage boys to answer switchboards and handle office chores. It did not take long, how- ever, before the company realized that putting boys in charge of the phone system was like putting a rabbit in charge of the lettuce. Bell's chief engineer characterized them as "Wild Indians." In addition to being rude to customers and taking time off without permission, the boys played pranks with switch- board plugs. They disconnected calls and crossed lines so that people found themselves talking to strangers. A similar phenomenon took place in the United Kingdom. A British commentator remarked, "No doubt boys in their teens found the work not a little irksome, and it is also highly probable that under the early conditions of employment the adventurous and inquisitive spirits of which the average healthy boy of that age is possessed, were not always conducive to the best attention being given to the wants of the telephone subscribers." 1

Teenage boys-and some girls too-have always been driven by a passion for adventure, so it is not surprising that those with an interest in technology would find phone systems, and later computers, an irresistible playground. These technologies offered endless opportunities for exploration and playing pranks-even venturing into the underworld of crime and espionage. Adopting "handles" (names) such as Phiber Optik, Dark Avenger, and Erik Bloodaxe, the young hackers played in the realm of fantasy while hiding behind a cloak of anonymity.

With the new technologies, hackers found a virtual playground that spanned the globe. With just a computer and modem, they could talk to and collaborate with other hackers on the opposite side of the world. They could penetrate computers in foreign countries and hop from one country to the next through global networks that tied the machines together. And indeed they did. Australian hackers met their British colleagues on a computer in Germany to discuss where to stash a file they had stolen from a machine in the United States.2 U.K. hackers penetrated systems in South America and the United States on their way to the Atomic Research Institute in South Korea.3

This book uses the word "hackers" to refer to persons who gain access to or break into electronic systems, particularly computers and telecommunications systems. This includes "crackers," who break access codes and computer locks, and "phreakers," who crack and exploit phone systems. The word hacker has a much broader-and nonpejorative-meaning, however, which includes any

computer enthusiast who likes to tinker with and program the machines. Most of these people do not engage in or condone illegal activity. They are expert programmers and network wizards who build systems and find and repair their flaws.

Some people object to using "hacker" to denote those who illegally break into systems, especially those who exploit tools with little knowledge of or apparent interest in how they work. They say such people are crackers, not hackers. I have chosen the word hacker because the people studied here call themselves hackers and refer to their activity as hacking. They write articles with titles such as "How to Hack XYZ." This terminology was picked up by victims, by investigators and prosecutors examining the evidence of their illicit acts, by scholars studying the computer underground, and by journalists reporting on the activity.

Breaking into systems is not always illegal. It can be done against one's own computers or against others with permission, for example, to expose vulnerabilities so they can be repaired. Sometimes the term "white hat" is used to refer to those who hack under these conditions. White hats are contrasted with "black hats," who penetrate other people's systems without permission, often for profit or malice.

Although this section focuses on hackers in their teens and early twenties whose activity has an element of play, not all hackers are teenagers. A survey of 164 hackers conducted by Professor Nicholas Chantler of Queensland University of Technology in Brisbane, Australia, found that their ages ranged from 11 to 46 years. Most, however, were between 15 and 24 years of age. Only 5% of the hackers surveyed were female.4

Motivation

Young hackers are motivated by a variety of factors, including thrill, challenge, pleasure, knowledge, recognition, power, and friendship. In the words of one former hacker I interviewed in 1990:

Hacking was the ultimate cerebral buzz for me. I would come home from another dull day at school, turn my computer on, and become a member of the hacker elite. It was a whole different world where there were no condescending adults and you were judged by your talent. I would first check in to the private bulletin boards where other people who were like me would hang out, see what the news was in the community, and trade some info with people across the country. Then I would start actually hacking. My brain would be going a million miles an hour and r d basically completely forget about my body as I would jump from one computer to another trying to find a path into my target. It was the rush of working on a puzzle coupled with the high discovery many magnitudes

> *intensified. To go along with the adrenaline rush was the illicit thrill of doing something illegal. Every step I made could be the one that would bring the authorities crashing down on me. I was on the edge of technology and exploring past it, spelunking into electronic caves where' I wasn't supposed to be.5*

In *SPIN* magazine, reporter Julian Dibbell speculated that much of the thrill came from the dangers associated with the activity, writing that "the technology just lends itself to cloak-and-dagger drama, ...hackers were already living in a world in which covert action was nothing more than a game children played."6

For one teen who went by the name Phantom Dialer, the ability to penetrate computers meant belonging to an elite group of people who could go anywhere and everywhere effortlessly in the global network. By the time he was caught, he had invaded hundreds and possibly thousands of computers on the Internet, including systems at military sites and nuclear weapons laboratories, bank automated teller machine (ATM) systems, systems belonging to For- tune 100 companies, and dam control systems. When asked if he had ever found a system he could not penetrate, his response was "No." It was not so much brilliance or skill that led to his success, but an incredible persistence.7

For an Australian hacker who called himself Anthrax, hacking meant power and a sense of control. Once he acquired access to a privileged account on a system, it was his to do with as he liked. He could run whatever programs he wanted. He could toss users off at will.8

Matthew Bevan, a hacker in England who went by the name Kuji, described the experience thus: 9

> *It is all about control, really. I'm in my little room with my little computer breaking into the biggest computers in the world and suddenly I have more control over this machine than them. That is where the buzz comes from. Anyone who says they are a reformed hacker is talking rubbish. If you are a hacker, you are always a hacker. It's a state of mind.*

Like many hackers, Bevan insisted his motive was curiosity, not personal gain. In giving his reasons for penetrating systems belonging to the U.S. Air Force, the National Aeronautics and Space Administration (NASA), and the defense con- tractor Lockheed, the ponytailed fan of the x- Files said, "I was after information about UFOs. I just wanted to find evidence of all the conspiracy theories-alien abductions, the 1947 Roswell landings and NASA faking the moon landings- and where better to look than their computer files?" 10

A hacker who used the code name Makaveli summed it up succinctly in an interview with AntiOnline: "It's power, dude. You know, power." The 16-year- old student from Cloverdale, California, had just received a visit from the FBI for allegedly hacking into unclassified U.S. Department of Defense computers.ll A

few months later, he and a 15-year-old neighborhood friend, called TooShort, pled guilty to federal charges of cracking Pentagon computers.l2

Makaveli and TooShort were mentored by an 18-year-old Israeli hacker named Analyzer.13 *Reuters* reported that Analyzer said he had broken into the Pentagon computers for the challenge but that he hacked Web sites operated by neo-Nazis, pedophiles, and anti-Israeli groups because they disgusted them. "The neo-Nazis say threatening things against Jews and the pedophiles get plea- sure out of pictures of kids. They are very proud of their sites so what could be better revenge than destroying them?" he said}4 The attack against the Pentagon computers, called "the most organized and systematic attack the Pentagon has seen to date," 15 is discussed further in Chapter 8.

Chantler found that among the 164 hackers surveyed in his study, the three main reasons for hacking were (in decreasing order) challenge, knowledge, and pleasure, all of which are positive aspects beneficial to discovery learning. These accounted for nearly half (49%) of the reasons cited. Another 24% were attributed to recognition, excitement (of doing something illegal), and friendship. The remaining 27% were ascribed to self-gratification, addiction, espionage, theft, profit, vengeance, sabotage, and freedom.16 Paul Taylor identified six categories of motivators from his in-depth study of hackers: feelings of addiction, the urge of curiosity, boredom with the educational system, enjoyment of feelings of power, peer recognition, and political acts.17

Culture

Hacking is partly a social and educational activity. Hackers operate and hang out on Internet Web sites, e-mail distribution lists, chat channels (real-time message exchange), Web sites and FTP (File Transfer Protocol) sites, Usenet newsgroups (non-real-time discussion groups with message archiving), and computer bulletin board systems (on-line services, usually dial-up, providing electronic mail, chat, and discussion groups). They publish magazines, most of which are electronic. A March 1997 article in the *New York Times* reported that there were an estimated 440 hacker bulletin boards, 1,900 Web sites purveying hacking tips and tools, and 30 hacker publications. 18

These services and publications are used to trade tips and software tools for hacking and news about technology and hacking. They feature "how to" guides for breaking into computer systems, evading detection, stealing phone services and listening in on calls, and cracking TV scramblers and other locks. They offer programs and command scripts for cracking passwords, locating and exploit - ing security holes on the Internet, and writing computer viruses. Hackers can download and run the software without even understanding how it works. Although many of these sources are geared toward hackers, they are read by

security specialists and investigators who want to keep track of the latest information circulating in the computer underground.

Hackers organize and attend conferences allover the world, where they get together to brag, swap war stories, exchange information, have fun-and crack codes. At the 1997 DefCon in Las Vegas, hackers attending the annual gathering were quick to penetrate the hotel's antiquated phone system. By the time the conference began, they had distributed instructions on how to call long distance free. This was not your usual crowd of conference goers. One attendee tried to pass counterfeit $20 bills when registering.19

The first hacker publication began as a newsletter called the *Youth Inter- national Party Line (YIPL),* founded in 1971 by Yippie activist Abbie Hoffman and AI Bell. The newsletter, which combined politics and technology, promoted phone phreaking while protesting the charges of what was then a monopolistic phone company. Hoffman wrote, "Obviously one reason for publishing *YIPL* has to do with free speech. Free speech like in 'Why should anyone pay for talking' and Free speech like in 'Why shouldn't anyone be allowed to print any kind of information they want including how to rip off the phone company'." Two years later, *YIPL* changed hands and its name to the *Technological American Party* (*TAP).* In 1979 it became the *TechnicalAssistance Program.* These changes brought on a more technical orientation. *TAP* died in 1984, but other magazines emerged to take its place. These included 2600: *The Hacker Quarterly,* named after the tone generated by phreakers to get free access to long-distance toll trunks, and *Phrack,* an electronic publication whose name comes from "phreak" and "hack." 2600 was founded by Eric Corley, also known as Emmanuel Goldstein (the hero in George Orwell's 1984), who continues to edit the New York publication. *Phrack* has changed editors several times.2°

Many hackers collaborate, in some cases forming special clubs or groups with limited membership. Slightly more than half (52%) of the hackers surveyed by Chantler said they work in teams. More than a third (39%) indicated they belonged to a specialized hacker group. Of those, the majority (21 %) were connected to two groups worldwide: Crackers, Hackers an' Anarchists and the Inter- national Network of Crackers.21

One of the earliest hacking groups called itself the "414 club," so named because the members all resided in U.S. area code 414. The gang was suspected of breaking into more than 60 business and government systems in the United States and Canada, including the Memorial Sloan-Kettering Cancer Center, Security Pacific National Bank, and Los Alamos National Laboratory. It received national publicity in 1983 when *Newsweek* magazine ran a story on hackers, featuring 414 hacker Neal Patrick on the cover. Above the photograph of a half-smiling young man sitting before his TRS-80 computer was the taunting question, "Trespassing in the information age-pranks or sabotage?"22 Fifteen years later, that question is rarely asked. The general consensus is that any hacking,

without the permission of the resource owners or in violation of the law, is wrong.

For many years, the Legion of Doom was the premier hacking group. Founded in 1984 by Lex Luther and eight other hackers, it got its name from a group led by Superman's arch rival, Lex Luthor, in the cartoon series *Super- friends.* The LOD operated one of the first invitation -only hacking bulletin board systems. It would later operate subboards on other underground boards. Group members published an electronic magazine called the *LOD Technical Journal* with articles of interest to the hacking community. By 1990, 38 hackers were members or former members of LOD. Members retired for a variety of reasons, including loss of interest, college, and expulsion. Some were arrested and sentenced to jail.[23]

Members generally subscribed to the hacker ethic that breaking into systems and browsing through files was good as long as you did not do it for money and you did not cause damage. In " A Novice's Guide to Hacking," The Mentor wrote, "Do not intentionally damage *any* system." However, the guide goes on to tell the reader to alter the system files "needed to ensure your escape from de- tection and your future access"-an act that practically every system administrator I know would rate as damage. The guide concluded with, "Finally, you have to actually hack. ...There's no thrill quite the same as getting into your first system." But not all LOD members followed this ethic. A few were busted for credit card fraud.

I became interested in the LOD in 1989 when one of its retired members, Frank Drake, sent me a letter asking ifhe could interview me for his now defunct cyberpunk magazine *WO.R.M.* He enclosed a copy of the latest issue, and I was surprised to see an article describing material from my book *Cryptography and Data Security.* I had long been curious about the computer underground and so decided it might be a good opportunity to learn more. It was not without trepidation, however. Would he distort what I said? Would he hack into my computer and destroy my files? Would he somehow rip me off? He did none of these things, and after the interview we switched sides so I could interview him.[24] I would then go on to interview other hackers as part of a research project on the computer underground.

Some hacking groups use their skills to combat pedophiles and child pornographers. StRyKe, a 25-year-old hacker with the U.K.-based Internet Combat Group (IGC), says, "I do think of myself as 'moral.' The traditional image of a hacker is no longer a valid one. I don't attack anyone who doesn't deserve it. We are talking about people who deliberately harm minors." The hackers trace the identity of pedophiles, attack their computers, and remove the pictures they post. Although the activity of the IGC and similar groups such as the American- based Ethical Hackers Against Pedophilia is illegal, police are said to accept in- formation given to them by the hackers.[25]

Some of the older, retired hackers believe that the hacking culture has de- generated. In his last column as *Phrack* editor, Eric Bloodaxe, a founding member of the LOD, wrote:

> *I don't like most of you people. ...People might argue that the community has "evolved" or "grown" somehow, but that is utter crap. The community has degenerated. ...The act of intellectual discovery that hacking once represented has now been replaced by one of greed, self- aggrandization and misplaced post-adolescent angst. ...I'm not alone in my disgust. There are a bunch of us who have reached the conclusion that the" scene" is not worth supporting; that the cons are not worth at- tending; that the new influx of would-be hackers is not worth mentoring. "'Maybe a lot of us have just grown Up.*[26]

More Than Child's Play

Many hackers, perhaps most, do grow up, stopping at age 18 when they can be prosecuted as an adult. But others keep going, and some are not content with breaking locks, acquiring knowledge, and roaming the infobahn. They engage in serious acts of fraud and sabotage, and the entire underground culture supports their activities. It is not unusual to hear of hackers trafficking in stolen credit card numbers ("carding") and pirated software ("warez"), sprawling graffiti on Web sites, and taking down Internet service providers. Hackers download proprietary and sensitive documents and snoop through e-mail. One group of hackers allegedly wiped out data on the Learning Link, a New York City public television station computer serving hundreds of schools.[27] Even hackers who do not intentionally cause harm typically alter system files and delete log entries to cover up their tracks and enable reentry. Considerable time and effort are required to clean up the files and restore the integrity of the system. In some incidents, victims estimated their cleanup and recovery costs to be several hundreds of thousands of dollars.

Computer hackers have penetrated systems in both the public and private sectors, including systems operated by government agencies, businesses, hospitals, credit bureaus, financial institutions, and universities. They have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning (OAM&P). They have crashed or disrupted signal transfer points, traffic switches, OAM&P systems, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs, disrupted emergency 911 services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan. They have attacked private branch exchanges and corporate networks as well.[28] They have installed wiretaps, rerouted phone calls, changed the greetings on voice mail systems, taken over voice mailboxes, and made free long -distance calls at their victims' ex - pense-sticking some victims with phone bills in the hundreds of thousands of dollars. When they cant crack the technology, they use "social engineering" to con employees into giving them access.

Hackers exploit weaknesses in laws as well as vulnerabilities in technology and human frailty. Juveniles are generally immune from federal prosecution, and in some countries hacking is not a crime. Foreign hackers may be immune to extradition. Analyzer, the Israeli hacker who broke into Pentagon computers, was protected by a treaty that prohibits extradition of Israeli citizens to the United States. The 18-year-old teenager did spend ten days under house arrest, however, while the FBI and Israeli police carried out their investigation.[29]

As of summer 1998, only one juvenile hacker has been prosecuted under federal law in the United States. On March 10, 1997, the hacker allegedly penetrated and disabled a telephone company computer that serviced the Worcester Airport in Massachusetts. As a result, telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service, and various private airfreight companies was cut off for six hours. Later in the day, the juvenile disabled another telephone company com- puter, this time causing an outage in the Rutland area. The lost service caused financial damages and threatened public health and public safety. On a separate occasion, the hacker allegedly broke into a pharmacist's computer and accessed files containing prescriptions. Pursuant to a plea agreement, the juvenile was sentenced to two years' probation, during v\Thich time he may not possess or use a computer modem or other means of remotely accessing a computer, must pay restitution to the phone company, and must complete 250 hours of community service.3°

As the Worcester case so vividly illustrates, hacking is more than child's play. It has serious implications for public safety and national security. If one teenager can disrupt vital services for hours, what might a terrorist organization or hostile government be able to accomplish? How many of these young hackers will grow up to be information thieves and terrorists- or sell their services to organized crime and terrorist organizations? How many terrorists will learn their skills by hanging out in the computer underground?

The Centre for Infrastructural Warfare Studies estimated in December 1997 that there were fewer than 1,000 professional hackers worldwide at the time. They defined "professional hacker" as someone who "is capable of building and creating original cracking methods. He has superior programming skills in a number of machine languages and has original knowledge of telecommunications networks. In terms of objectives, his goals are usually financial." [31]

One group of hackers, called the LOpht (pronounced "loft"), formally banded together in 1992 to acquire a lease to a warehouse in Boston. Now in their twenties and thirties, with jobs and wives, the hackers retreat at night to a warehouse in Boston, where they probe software for security flaws and post what they find on the Internet. One member, who goes by the name Mudge, says that "We think of our Net presence as a consumer watchdog group crossed with public television. ...At this point, we're so high profile. ..it would be ludicrous for us to do anything wrong." The *Washington Post* characterized the LOpht as "white hat" hackers. "Even companies whose products have been hacked for security weaknesses laud the social ethos and technical prowess of the members of the LOpht," the *Post* reported. Microsoft, for example, took LOpht members to dinner and has worked with them to plug security loopholes in their products.32 In May 1998, LOpht members testified before the u.s. Senate on the state of security on the Internet. They said they could bring down the foundations of the Internet in 30 minutes by interfering with the links between long-distance phone carriers.33

CRIME

The second domain of information warfare is that of crime. Although the activities described in the previous section are generally illegal, they were treated separately because most teenagers operate with a different level of maturity and with different motives than other criminal players, who are motivated primarily by money.

The following sections summarize criminal activity in two areas: intellectual property crimes and fraud. Many of the other criminal acts covered in this book fall in the area of sabotage of information resources.

Intellectual Property Crimes

Crimes against intellectual property include piracy and theft of trade secrets. In- formation piracy involves the illegal acquisition and distribution of copyright materials, including images in electronic and print form; audio and video material stored on tapes, compact discs, and computers; and software stored in computer files and distributed on disk. Although some pirates are teenage hackers and ordinary citizens, there is a substantial criminal element that seeks to profit from the mass production and sale of pirated goods. In 1996, the major U.S. copyright industries lost an estimated $18 billion to $20 billion in revenue be- cause of piracy outside the United States, according to the International Intellectual Property Alliance. Domestically, the estimated losses exceeded $2.8 billion.34 Information piracy also includes the misappropriation of trademarks. Theft of trade secrets involves the unauthorized acquisition of a company's trade secrets. It is conducted by domestic and foreign competitors and by foreign governments who spy on behalf of their industries. Insiders frequently are involved. Sometimes they walk off with their employers' secrets to start competing firms.

Based on their 1997/98 survey of Fortune 1000 and the 300 fastest growing companies in the United States, the American Society for Industrial Security (ASIS) estimated that the total annual dollar losses to U.S. companies from intellectual property theft may exceed $250 billion. The survey itself identified 1,100 documented incidents and $44 billion worth of intellectual property targeted in a 17 -month period. In addition, nearly 50% of respondents reported suspected losses but could not document them. The most frequent targets were high-tech companies, particularly in Silicon Valley, followed by manufacturing and service industries. Targeted information included research and development strategies, manufacturing and marketing plans, and customer lists.35

The ASIS survey also confirmed what information security experts have been saying for years, namely that the highest risk groups for corporate trade secrets include former employees, temporary staff, current employees, vendors or suppliers, and consultants. The 1996 survey reported a similar result. Other identifiable threats include hackers, domestic and foreign competitors, foreign intelligence services, and foreign business partners.36 The top five countries cited as risks were the United States, China, Japan, France, and the United Kingdom. Significant increases were reported for other countries including Mexico and Russia.37 Kenneth Rosenblatt, deputy district attorney for Santa Clara County, California (Silicon Valley), reports that the vast majority of information thieves are competitors, however, not foreign governments.38

Prior to 1996, theft of trade secrets was not explicitly addressed by federal law in the United States. Prosecutors had to apply laws designed for other purposes, including wire fraud,[39] mail fraud,[40] interstate transportation of stolen goods,[41] and interstate receipt of stolen goods.[42] Alternatively, they could prosecute under state trade secret laws, which emerged in the *1970s.*[43] The laws were inadequate, however, and some thieves went free.

In 1996, Congress passed the Economic Espionage Act of 1996 to provide stronger trade secret protection at the federallevel.[44] The law made it illegal for anyone to knowingly steal or otherwise fraudulently obtain a trade secret, to copy or distribute a trade secret, to receive or buy a trade secret, or to attempt or conspire to commit one of these acts in order to benefit a foreign government, instrumentality, or agent or to convert the trade secret to the economic benefit of anyone other than the owner. Penalties can be as high as $10 million and 15 years in prison for acts conducted to benefit a foreign government, instrumentality, or agent (economic espionage) and $5 million and 10 years in prison for acts conducted to benefit other parties (commercial espionage) .For the purposes of the law, "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information provided the owner has taken

reasonable measures to keep such information secret and the information derives independent economic value, actual or potential, from not being generally made public.

Not all information warfare operations against intellectual property are of a criminal nature. Businesses regularly gather intelligence about their competitors from open sources, including public records, Internet documents, trade shows, and Freedom of Information Act (FOIA) requests. Although sensitive information might be deduced from open sources, this method of collection is perfectly legal.

Fraud

Crimes in this category include telemarketing scams, identity theft and bank fraud, telecommunications fraud, and computer fraud and abuse. Examples of others are presented in later chapters. In principle, any type of fraud might be considered information warfare as it degrades the integrity of some information resource to the advantage of one party and the disadvantage of another. Not all of these areas are treated in this book, however, in part because the book would become too big.

With telemarketing fraud, the huckster gains access to some medium, typically the telephone, postal mail, e-mail, or the Web, and corrupts its integrity by injecting messages offering phony deals. Victims part with their credit card numbers and checks drawn against their accounts in exchange for bogus prize money, phony offers, and "get rich quick" promises. According to Neil Gallagher of the FBI's criminal division, Internet scams were becoming "epidemic." One pyramid scheme, called Netware International, had recruited 2,500 members with promises of profit sharing in a new bank that was to be formed.[45] Telemarketing fraud is estimated to cost U.S. consumers $40 billion a year, making it the costliest form of information warfare after intellectual property theft.[46]

Identity theft involves gaining access to another person's identifiers such as name, social security number, driver's license, and bank and credit card numbers. The thief then takes actions in the owner's name such as withdrawing funds, charging purchases, and borrowing money. In so doing, the victim's bank and credit records become corrupted with damaging information that has nothing to do with the victim's behavior. The criminal gains from the impersonation, while the victim and card issuers suffer monetary and other losses. Some victims' lives become a nightmare as they try to reestablish credit and get their records corrected. In the United States, individual liability is limited to $50 for credit card abuse, but Visa and MasterCard have indicated that their member banks lose hundreds of millions of dollars annually from identity theft.[47]

Many Internet users worry that thieves will get their credit card numbers by intercepting their Web transactions. In practice, however, the thieves get the numbers by other means. They raid mailboxes and trash bins, bribe insiders, and hack into the computer systems where they are stored. Increasingly, Web trans- actions are encrypted (scrambled), so even if they are intercepted, an eavesdropper will get only gibberish. There have been no reported incidents of thieves collecting credit card numbers by intercepting encrypted Web communications even when the encryption used was not considered strong.

Most identity theft involves some sort of bank fraud. In some cases, the fraud is against a corporate account and involves the fabrication of million- dollar transactions against the account. Although such acts are usually committed by insiders, there have been a few reported cases of outsiders gaining unauthorized access to financial systems, most notably the case of the Russian hacker who robbed Citibank computers in 1994.

When the case first came to light in September 1995, Vladimir Levin, a computer operator in St. Petersburg, had been accused of attempting to steal more than $10 million from large corporate accounts he had compromised on Citicorp's cash management system the preceding year.48 An investment company official for one of the victims, Investment Capital SA in Buenos Aires, signed on one day as the intruder was transferring $200,000 from its accounts into unknown bank accounts in San Francisco. Company officials notified Citicorp, which had already seen $400,000 disappear through accounts in San Francisco and Finland. This time they were prepared. They alerted the San Francisco banks, which froze the accounts, and the FBI, which arrested a woman by the name of Katerina Korolkov after she tried to withdraw the funds. From Korolkov and her husband, Evgueni, officials learned that the hacker worked out of an office of the St. Petersburg software company AO Saturn. They obtained further intelligence from another accomplice, Vladimir Voronin, whom they caught as he tried to withdraw more than $1 million from a bank in Rotterdam. Voronin admitted he had recruited "mules" to collect cash after it had been illegally transferred. U.S. authorities then enlisted the aid of Russia's Organised Crime Squad, which helped them acquire evidence from phone company records that the calls were coming from Levin at AO Saturn. However, lacking a wire fraud statute and extradition treaty with the United States, the Russians could not arrest him. They had to wait until Levin traveled outside the country. On March 2, 1995, Scotland Yard's extradition team arrested Levin as he stepped off a plane at Stansted air- port, north of London. After fighting extradition to the United States, he was finally transferred to a prison in upstate New York on September 1997. In Janu- ary 1998, Levin pled guilty to transferring $3.7 million from customer accounts to accounts he and his accomplices controlled at banks in Finland, the Nether- lands, Germany, Israel, and the United States. Now 30, he was sentenced to three years in prison and ordered to make restitution to Citibank for $240,015.49

The attack against Citibank illustrates the complexities of investigating and prosecuting crimes that exploit global information infrastructures, which move

money around the world and provide remote access from anywhere at any time. Successful resolution of these cases can hinge on the laws of the countries in which the criminals operate and on the cooperation of the law enforcement agencies in those countries. Before it was over, the Citibank case involved more than a dozen different countries.

In the area of telecommunications fraud, criminals acquire and sell long-distance telephone services. They eavesdrop on cellular communications, pick up the numbers of the phones, and program the numbers into "cloned" phones, which bill to the victims. Then they set up call selling operations, making a profit from the stolen service. U.S. cellular carriers lost approximately $1 billion to cellular fraud in 1996.50 The total losses from all phone fraud in the United States were estimated to be about $8.9 billion in 1992. Employees were the biggest threat, generating estimated losses of $5.2 billion.51

Credit card and telecommunications fraud are instances of superimposition fraud, which involves superimposing unauthorized usage of an account on top of another party's legitimate usage. Charges for the stolen service are made against the pilfered account. Computer fraud is another form of superimposition fraud.

Computer Fraud and Abuse

Computer fraud and abuse involve accessing computers without authorization, exceeding authorization, and performing malicious acts against computing re- sources. Specific types of activities include accessing and downloading sensitive information, initiating bogus transactions, tampering with records, disrupting operations, and destroying files or equipment. These activities give the perpetrator greater access to sensitive information while diminishing the integrity of the systems compromised or denying service. The perpetrator can be an outside hacker or thief or an insider who misuses access privileges. Damages resulting from tampering and lost service sometimes run in the hundreds of thousands of dollars. One employee ruined company morale and almost drove his employer to bankruptcy before finally being caught after a six-month rampage (see Chapter 6).

Computer crime and misuse have been on the rise, no doubt owing to the proliferation of computing technologies and growth of the Internet. The Federal Bureau of Investigation reported a significant increase in pending cases, from 206 in 1997 to 480 in 1998.52

In 1996, the Computer Security Institute (CSI) and FBI began conducting an annual survey of computer security practitioners. In 1998, 64% of the 520 respondents reported unauthorized use of computer systems within the past 12 months. This was up from 50% of 563 respondents in 1997 and 42% of 428 respondents in 1996. The numbers could be even higher, as 18% reported that they were unsure if their system had been misused. Inside attacks were somewhat more common than outside attacks, with 36% reporting one or more incidents of insider misuse as compared with 28% for incidents involving outsiders. Only 17% said they reported cases to law enforcement. The survey also showed that the Internet is increasingly a source of problems, with 54% citing Internet access as a frequent point of attack or misuse in 1998 as compared with 47% in 1997 and 38% in 1996.53

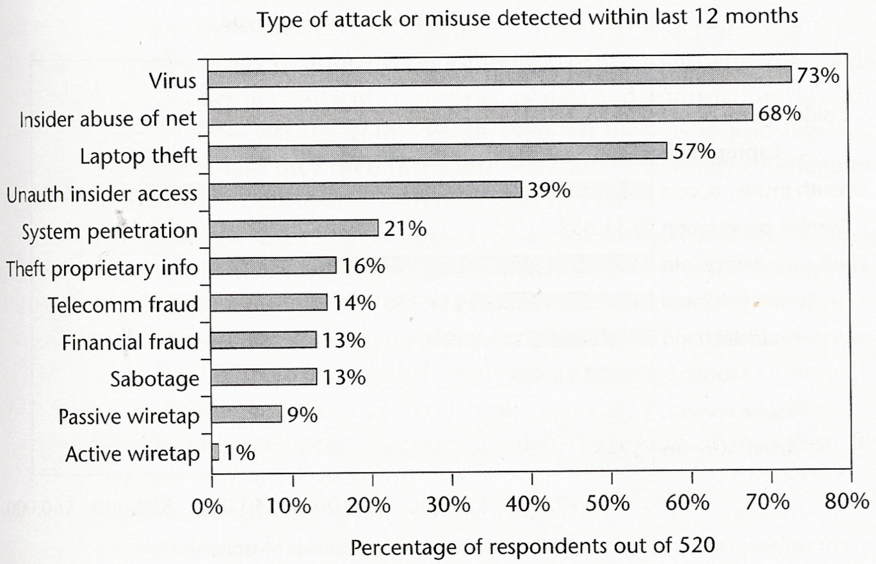

FIGURE 3.1. Types of attacks or misuses reported in the 1998 CSI/FBI Computer Crime and Security Survey.

About three quarters of respondents reported suffering financial losses from computer security breaches in 1997 and 1998. Not all organizations could quantify their losses, but of those that could, the combined losses exceeded $136 million in 1998 compared with $100 million in 1997. Two thirds or $90 million of the 1998 losses was attributed to three significant incidents. One company re- ported a $50 million loss from unauthorized insider access. Another said it lost $25 million through theft of proprietary information. A third claimed a $15 mil- lion loss from telecommunications fraud. In addition, there were at least five other incidents with reported losses of $1 million or more, including a $2 million loss from financial fraud and a $2 million loss from viruses. By comparison, in 1997 the largest single incident (telecommunications fraud) accounted for a $12 million loss and the second largest (theft of proprietary information) $10 mil- lion. None of the others exceeded $2 million. Thus, the overall increase in financial losses from 1997 to 1998 does not imply that most companies are suffering greater financial losses, as the data are heavily skewed by a few major incidents.

Figure 3-1 shows the number of respondents reporting different types of attacks or misuse against their computing and telecommunications resources,

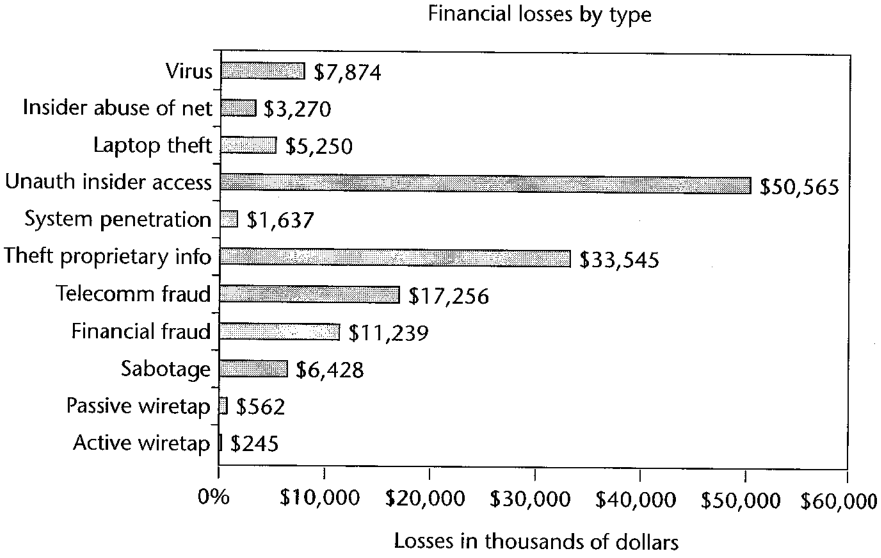

FIGURE 3.2. Total financial losses reported in 1998 CSI/FBI Computer Crime and Security Survey for incidents with quantifiable losses.

ordered from most prevalent to least prevalent type. Figure 3-2 shows the losses in thousands of dollars for incidents of those types with quantifiable losses. The figures show that whereas computer viruses were encountered by the greatest number of companies, with 73% of respondents saying they detected incidents of that type, they did not account for the largest losses, which were attributed to unauthorized access by insiders and theft of proprietary information. The two least reported threats, active and passive wiretaps, however, also accounted for the smallest losses. The respondents said that likely sources of attack are disgruntled employees (89%), independent hackers (72%), U.S. domestic corporations (48%), foreign corporations (29%), and foreign governments (21%).

There have been several other studies of computer-related crimes. *Information Week* and Ernst & Young completed their fifth annual survey of information security and information technology managers in 1997. Of the 627 U.S. respondents to the 1997 survey, 43% reported malicious acts from employees, compared with 29% in 1996, and 42% reported attacks from outsiders, com- pared with 16% in 1996. There was a significant growth in reported cases of industrial espionage, with 38% saying they had been victims in 1997, compared with only 6% in 1996. Almost 60% cited lack of money as an obstacle to addressing security concerns.54

WarRoom Research, LCC conducted an information systems security survey of Fortune 1000 + firms in 1996 and again in 1998. Their 1998 survey found that the vast majority of companies had been attacked by outsiders. Almost 60%

of those reported losses greater than $200,000. Further, 69% of respondents said they had been the target of information espionage, which they defined as "a directed attempt to identify and gather proprietary data and information via computer networks." This was up from 53% in 1996. Of those who said they had been targeted, 68% said they used intrusion detection technology to safeguard their networks in 1998, compared with only 27% in 1996.55

In Australia, the Office of Strategic Crime Assessments and the Victoria Police Computer Crime Investigation Squad mailed 310 surveys to a representative sample of companies in 1997. Of 159 responses, 37% reported some form of computer intrusion or misuse during the past 12 months. The attacks were attributed most frequently to disgruntled employees (32%) and criminals or hackers (21 %). Respondents did not perceive competitors, customers, suppliers, or foreign government intelligence agencies as high-risk groups. Motivation for the breaches was attributed to curiosity (49%), espionage (26%), financial gain (10%), extortion/terrorism (10%), and malicious damage (4%). Seventy-seven percent estimated their direct and indirect losses as under $10,000 per incident. Only 6% reported losses over $100,000.56

In the United Kingdom, a 1997 study conducted by the Audit Commission found that of900 responses, 45% reported incidents of computer fraud or abuse. This was up from 36% in 1994. Fraud accounted for 13% of all computer-related incidents, hacking for 8%.57

India's National Centre for Research in Computer Crimes reported that the number of serious computer crime cases reported to them had doubled each year since 1991, with 50 reported cases in 1996 -1997. They estimated that this represented 10% to 20% of the total. Over 65% of the crimes were committed against financial institutions, 28% against manufacturing companies.58

Fighting Crime

Information warfare operations are used not only to commit crime but also to fight it. Law enforcement agencies use visual and electronic surveillance, including wiretaps and bugs, to collect evidence and intelligence in criminal investigations. They use informants to get access to inside information. They corrupt the integrity of their target's information space through undercover operations and stings.

The criminals fight back, using their own offensive and defensive information warfare techniques against the police. They use surveillance tools to watch the police and concealment technologies to hide from them. They use psychological operations to destabilize the police. Some organized crime groups have hired hackers to assist them with information warfare offense and defense.

Drug cartels are said to be spending a fortune on the latest technology to spy on and elude law enforcement. At a four-day conference in 1997, one Drug Enforcement Administration (DEA) agent was quoted as saying, "Drug traffickers have the best technology that money can buy. And they hire people from the intelligence community in some countries to operate it for them or teach them how to use it." They intercept phone calls, set up electronic surveillance inside trucks, and encrypt their cellular phone calls.59

Dutch organized crime offers an interesting case study in the use of information warfare. The gangsters have their own information warfare division that combines muscles, brains, know-how, guts, and money to achieve their goals. The division works for anyone willing to pay them. They work in cell structures, loosely coupled and hard to get. The Amsterdam police faced severe information warfare attacks when investigating two major drug organizations, known as the cases of "Charles Z." and "De Hakkelaar." The criminals were found tapping the phone lines of safe houses and the homes of high police officials. They broke the analog encryption used by many Dutch government services. They built receivers to monitor nationwide pager networks. Intercepted information was fed into a database, where it was further processed to determine, for example, which special units were cooperating with each other. The criminals burglarized the houses of district attorneys and police officers. They spread rumors to discredit DAs and the investigation. They stole PCs and diskettes, publishing their con- tents during the trials. In short, everything was done to obstruct justice and the trials, although some were convicted anyway.60

Dutch organized crime has used encryption in its attempts to evade law enforcement. It has received technical support from a group of skilled hackers who themselves used PGP (Pretty Good Privacy) and PGPfone to encrypt their communications. The hackers at one time supplied the mobsters with palmtop computers on which they installed Secure Device, a Dutch software product for encrypting data. The palmtops served as an unmarked police-intelligence vehicles database.

INDIVIDUAL RIGHTS

The third domain of information warfare covers conflicts over individual rights, particularly rights to privacy and free speech. These conflicts arise between individuals, between individuals and businesses, and between individuals and their governments. They are age-old conflicts that are likely to be with us forever. In- deed, they are aggravated by new information technologies, which offer new opportunities for both privacy and surveillance and for both information dissemination and information control. In so doing, they can facilitate both offensive and defensive information warfare operations and both crime and crime prevention.

Conflicts between individuals over free speech arise when the speech of one party is harmful or disturbing to another. An example is one person defaming another in a public forum, such as on the Internet. The effect is to corrupt the forum with lies that are damaging to the person defamed. Other examples include ."flaming" (making insulting and derogatory remarks about others, often in a public forum), sending threatening or harassing messages, and bombarding a person's e-mail box with thousands of messages. In the area of privacy, conflicts arise when one person spies on another, for example, by eavesdropping on the person's phone calls, or reveals confidential information about the person to a third party. Whereas many areas of conflict are protected by laws (and thus fall in the domain of crime as well as rights), others are not.

Information warfare between individuals and businesses in the area of free speech typically involves the theft and distribution of intellectual property. Many hackers, for example, subscribe to the principle that "information ought to be free," meaning that they should be able to access and share computing and telecommunications resources, including software, at will and usually without paying. The principle does not apply to all types of information, for example, confidential information about individuals, although many hackers help them- selves to that as well. Also, as noted earlier in this chapter, hackers-even some of the "white hats"- believe they should be able to publish software that exploits computer vulnerabilities no matter what the consequences are to the organizations that rely on those systems to manage their critical assets.

In the area of privacy, many conflicts between individuals and businesses are related to the secondary use of information. Businesses sell or otherwise use customer information in ways that customers perceive violate their privacy and go beyond the reasons the information was collected in the first place. In becoming more available, the information may be used in ways that are detrimental to customer interests. Sometimes customers may not even realize the information was collected. Information warfare battles between individuals and businesses also occur over junk mail and e-mail, which clogs mailboxes and takes time to process.

Conflicts between individuals and governments in the area of speech arise over censorship. Governments exercise varying degrees of control over broad- cast media and the press. They outlaw certain types of speech, such as child pornography, independent of the medium. In some countries, they ban or control access to the Internet and satellite TV. The effect of these actions is to deny citizens access to certain types of information or media. Publishers are also denied access to particular media. The rationale is that censorship is needed to pro- tect national interests. A big issue in the

United States and elsewhere has been whether certain types of speech on the Internet should be prohibited in order to protect children.

With respect to privacy, there is contention over government surveillance of citizens, in particular the conditions under which a government agency is allowed to intercept communications or search and seize documents and computers and the degree to which technology should be regulated to make government access possible. This is an information warfare issue because the outcome determines the extent to which the government can get access to the information resources of a citizen when it is not in the citizen's interest to provide that access, for example, because the person has committed a crime.

In the United States, there is general agreement about the conditions for government access to private communications and files-a court order based on probable cause of criminal activity. But there is considerable disagreement over whether technologies should be controlled to facilitate that access. An area of particular contention is encryption technology, which has been subject to export controls but not domestic regulation.

NATIONAL SECURITY

-

The fourth domain of information warfare covers operations undertaken by states and by nonstate players against states. These include foreign intelligence operations, war and military operations, acts of terrorism, and netwars. Although acts of terrorism and netwars need not occur at a national level, they are de- scribed here because they often do.

Foreign Intelligence

When Henry L. Stimson learned in 1929 that the United States was reading Japan's diplomatic cables, he was irate. "Gentlemen," the secretary of state brusquely declared, "do not read each other's mail." But by 1941, when U.S. codebreakers were handing him dispatches revealing Japanese war moves, Stimson had changed his view. Now secretary of war, he noted in his diary the spies' "wonderful progress." 61

It is probably fair to say that every country has an intelligence branch or unit that gathers information about foreign allies and adversaries, including for- eign governments, terrorist organizations, and other threats to national security. This information is acquired not only during times of war but also during times of peace, with the objective of protecting national interests. Although much of the information that is collected is obtained through open channels, some is acquired covertly through human spies and electronic surveillance, perhaps even computer hacking.

The intelligence priorities of the United States and Japan offer a glimpse into the role of foreign intelligence. In a speech to staff members of the Central Intelligence Agency (CIA), President Clinton defined the priorities of the u.s. intelligence community: (1) the intelligence needs of the military during an operation; (2) political, economic, and military intelligence about countries hostile to the United States and all-source information on major political and economic powers with weapons of mass destruction who are potentially hostile to the United States; and (3) intelligence about specific transnational threats, such as weapons proliferation, terrorism, drug trafficking, organized crime, illicit trade practices, and environmental issues of great gravity.62

The priorities of Japan's intelligence system, at least in the late 1980s, were documented in a 1987 CIA report on Japanese foreign intelligence and security services. They included information pertaining to (1) access to foreign sources of raw materials; (2) technological and scientific developments in the United States and Europe; (3) political decision making in the United States and Europe, particularly as it relates to trade, monetary, and military policy in Asia and the Pacific region; and (4) internal political and military developments in the then Soviet Union, China, and North Korea. The report concluded that about 80% of assets were directed toward the United States and Europe, concentrating on high technology. The Ministry for International Trade and Industry (MITI), the Japanese External Trade Organization (JETRO), and multinational corporations such as Hitachi and Mitsubishi were said to playa critical role in intelligence gathering.63 Ben Venzke, publisher of the *Intelligence Report,* said that "In Japan the underlying philosophy is, why spend 10 years and $1 billion on research and development when you can bribe a competitor's engineer for $1 million and get the same, if not better, results?"64

Governments increasingly target economic information and trade secrets in order to protect or boost their economies. According to the FBI and Defense Investigative Service (DIS), the primary targets within the United States are high-technology and defense-related industries. By acquiring advanced technologies, foreign countries can develop leading-edge weapons systems and other products without spending the time or money on research and development. Areas of foreign collection activity and interest include biotechnology, chemical and biological systems, computers, information systems, telecommunications, information warfare, sensors and lasers, electronics, semiconductors, manufacturing, materials, energy, nuclear systems, aeronautics, space, marine systems, and weapons.65

As of May 1997, the U.S. counterintelligence community had identified suspicious collection and acquisition activities of foreign entities from at least 23 countries during the past year. Of these, 12 were singled out as most actively targeting U.S. trade secrets. These countries are said to use clandestine and ille- gal methods as well as overt and legal ones.66 In the two-year period following the inception of their Economic Counterintelligence Program in 1994, the Federal Bureau of Investigation observed a 100% increase in the number of suspected

economic espionage cases under investigation-from 400 to 800 cases.67 As of January 1998, more than 700 cases were said to be pending before the bureau.68

In February 1996, FBI Director Louis Freeh testified that the January 1995 issue of *Law and Policy in International Business* stated that the White House Office of Science and Technology estimated nearly $100 billion in annual losses to U.S. businesses from foreign economic espionage.69 In March, Freeh commented on the overall economic impact. "This is not a question of protection- ism. This is a question of the health and future of the American economy. The United States has become, in effect, the basic research laboratory of the world. The $249 billion we spend on research and development-both inside and outside the Government-goes into products that keep our economy strong and make us a market leader in many areas of the world. We are concerned about the impact on our economy-and our products-if we are to lose that leadership position."70

There is little information in the public domain about the use of computer hacking in foreign intelligence operations. According to Peter Schweizer's book *Friendly Spies,* Germany initiated one such program, dubbed Project Rehab after the harlot who helped the Israelites infiltrate Jericho, in the mid-1980s. The project was developed within Germany's intelligence agency, the Bundes Nacrichten Dienst (BND), as a joint effort between the BND's central office and the divisions for human and signals intelligence. The unit allegedly accessed computer sys- tems in the United States, the former Soviet Union, Japan, France, Italy, and Great Britain, and in 1991 penetrated the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, which carries most international bank transfers.71

Government intelligence agencies engage in information warfare for purposes other than information collection. For example, they create cover stories to conceal the true purpose of missions and use perception management to sway public opinion and win support for objectives in foreign countries.

According to *Federal Computer Week,* U.S. intelligence agencies are studying ways to use computers and the Internet to influence public opinion in the world's hot spots. Advanced software tools would be used to manipulate images and video so that a news clip, for example, might show the presence of a larger military force than is actually deployed in order to convince a world leader that a massive invasion is imminent.72

The use of perception management to trigger political change is not new. Intelligence agencies used leaflets and broadcasts in Iraq during the Gulf War, for example, as noted in Chapter 1. Unlike information in these other media, however, information posted on the Internet has a staying power. It will reach a broader audience, including American citizens, and ma)' have a longer term effect. This raises questions about oversight and regulation of information operations that exploit the Internet and about whether operations will introduce new

risks.73 To the extent that disinformation is posted on the Internet, the Net loses its value as a source of information. Everything becomes suspect.

War and Military Conflict

The opening section of this book on the Gulf War illustrates some of the ways in which information warfare has been used in a recent military conflict. But what will war be like in the future? Will it be mainly an information war? Will cyberspace troops of hackers replace conventional armed forces? Will it be bloodless?

There are several possible directions for the future. One is a continuation of trends seen in the Gulf War. Operations will exploit new developments in technology-particularly sensors and precision-guided weapons-but they also will make use of conventional armed forces and psyops and perception management. Information warfare will be an important strategic element of war- fare, but it will be accompanied by a strong showing of physical force, on the ground, at sea, and in the air. Intelligence operations, including the use of human spies as well as high-tech surveillance systems, will be critical. Military communications will be disabled or destroyed largely by physical weapons, not computer hacking, although cyber attacks may playa part in operations.

A second future scenario is a radical departure from current trends to one in which operations take place almost exclusively in cyberspace. Under this scenario, wars will be fought without any armed forces. Instead, trained military hackers will break into the enemy's critical infrastructures, remotely disabling communications, command, and control systems that support government and military operations. Operations might also target key civilian and commercial systems, such as banking and finance, telecommunications, air traffic control, and power supply. At present, however, there is no evidence to support the notion that a country's infrastructures could be so disabled by hacking that a government would surrender to a foreign power or alter its policies. The fallout from such an attack and how it would affect the decision-making systems of the enemy are unknown. Launching it would require considerable knowledge about target systems and interconnectivities. At least in the near term, the scenario re- mains largely in the realm of science fiction. Computer hacking, however, might be used as an accompaniment to other types of operations, as noted before.

A less radical scenario is one that uses a combination of advanced technologies and physical weapons but no ground forces. Scenarios of this type have been advanced within the U.S. military under the premise that through technological supremacy, all ground troops could be abjured in favor of precision weapons launched from remote platforms. Lieutenant General Paul Van Riper and Major Robert H. Scales Jr. dismiss the plausibility of such a scenario, however, arguing that it does not take into account the uncertainties and complexities of war or the lessons of history. "In addition to what history reveals about the

inherent nature of war, our own military experience in this century argues the contrary.:' They also point out that this is not the first time the military has been lured by promises of a high -tech, bloodless victory: "Recurring proposals to substitute advanced technology for conventional military capabilities reflect a peculiarly American faith in science's ability to engineer simple solutions to complex human problems." 74

Another radical scenario, at the opposite end of the spectrum, employs psyops and perception management in lieu of advanced weaponry. In an article titled "How We Lost the High-Tech War of 2007," Colonel Charles J. Dunlap Jr. presents the transcript of a fictitious address delivered by the Holy Leader of a non-Western country to his country's Supreme War Council in 2007. In that address, he explains how they engineered the defeat of America, which failed to heed a warning from one of its own army majors, Ralph Peters Jr., who wrote that in the future, America "will often face [warriors] who have acquired a taste for killing, who do not behave rationally according to our definition of rationality, who are capable of atrocities that challenge the descriptive powers of language, and who will sacrifice their own kind in order to survive." 75

The strategy of this fictitious country was to make warfare so psychologically costly that the Americans would lose their will to win. This was accomplished by committing one brutal act after another, all in front of global television. In so doing, they exploited the power of the medium to influence decision makers. They made extensive use of human shields, binding hostages to tanks and military vehicles. They induced the Americans to drop a small bomb on a biological warfare laboratory. Then, just as it was about to hit, they detonated their own nuclear bomb, killing 30,000 people in front of hundreds of millions of viewers who were watching the whole event live on TV. The world was shocked and held America responsible for the atrocity. Then they used their Boys Brigade to rape American women prisoners of war, amputating their limbs and burning their faces, but leaving them alive to return home in wheelchairs, horribly mutilated and shrieking in agony. Before America finally capitulated, the)T had attacked her homeland, planting bombs in facilities and parks where the elderly gathered, leaving needles infected with the human immunodeficiency virus (HIV) on beaches, and polluting coastlines by sinking oil tankers. Dunlap concludes that "cyber-science cannot eliminate the vicious cruelty inherent in human conflict." 76

War is likely to remain a gory business. Global television makes psyops and perception management, combined with staged brutality, a powerful force. Events in Rwanda, Burundi, and Zaire show that some of war's worst excesses-extreme brutality, mass slaughter, and intentional starvation-are all too common in parts of the world!7 High -tech gadgets and weaponry will not replace the loss of blood.

Although the future of war cannot be predicted, one thing seems certain: information warfare, in all its various manifestations from espionage and intelligence operations to electronic warfare to psyops and perception management, will play an important role, as it has throughout history. Some of the technologies may change, and with them specific methods, but the principles of acquisition, corruption, and denial of information resources will remain intact. Cyberspace no doubt will play some part, perhaps even strategically, but it will not become the only battleground.

So far, the rules and strategies for launching cyber attacks have yet to be defined. There are indicators, however, that some countries are exploring the application of cyber weapons and the legal, ethical, and operational consequences of employing them. The u.s. Department of Defense announced in March 1998 a proposed plan to establish a new deputy assistant secretary for Information Operations within the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The proposal would set up a directorate for offensive information warfare as well as one for defensive operations.78 According to the *Washington Post,* the government has considered using computer viruses and "logic bombs" to disrupt foreign networks and sow confusion, manipulating cyberspace to disable an enemy air defense network, shutting off power and phone service in major cities, feeding false information about troop locations into an adversary's computers, and morphing video images on foreign television stations.79

In their seminal paper "Cyberwar Is Coming!" John Arquilla, a professor at the Naval Postgraduate School in Monterey, California, and David Ronfeldt, an analyst at the RAND Corporation in Santa Monica, California, introduced the concept of "cyberwar" for the purpose of thinking about knowledge-related conflict at the military level: "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about one- self. It means turning the balance of information and knowledge in one's favor , especially if the balance of forces is not." Cyberwar can exploit modern technology, including sensors, computers, networks, and databases. At the same time, it does not require advanced technology. It is seen as a transformation in the nature of war that is about organization and psychology as much as technology. Adversaries will be organized more as networks than hierarchies, with decentralized command and control.8°

Terrorism

Terrorism refers to the actual or threatened use of violence with the intention of intimidating or coercing societies or governments. It can be conducted by individuals or groups and is often motivated by ideological or political objectives. Terrorists have traditionally employed two principal forms of information warfare: intelligence collection and psyops and perception management. Some groups have begun to exploit computing technologies to support these operations, for example, using the Internet to spread propaganda and a variety of on- line sources to collect information. In February 1998, Clark Staten, executive director of the Emergency Response & Research Institute (ERRI) in Chicago, testified before a U.S. Senate subcommittee that "even small terrorist groups are now using the Internet to broadcast their message and misdirect/misinform the general population in multiple nations simultaneously." He gave the subcommittee copies of both domestic and international messages containing anti- American and anti-Israeli propaganda and threats, including a widely distributed extremist call for "jihad" (holy war) against America and Great Britain.[81] In June, *U.S. News* & *World Report* noted that 12 of the 30 groups on the U.S. State Department's list of terrorist organizations are on the Web. Forcing them off the Web is impossible, because they can set up their sites in countries with free- speech laws. The government of Sri Lanka, for example, banned the separatist Liberation Tigers of Tamil Eelam, but they have not even attempted to take down their London-based Web site.[82]

Before the 1998 peace agreement, the Irish Republican Army was said to have developed a "sophisticated computerized intelligence bank using databases in the [Irish] republic, America and France." A sympathizer employed by British Telecom stole telephone billing records in order to determine the addresses of potential murder targets. The IRA also sifted through customer databases maintained by the private health care company BUPA and Thomas Cook's travel agents. The high-tech intelligence network was uncovered after authorities seized a batch of computer disks in Belfast. The disks included copies of the electoral register, which was used to find the names of police officers and other potential targets. The IRA used encryption to conceal their files, but the officers were able to decrypt the disks after months of effort.[83]

Other terrorist groups have used encryption as a defensive information warfare tool. Ramsey Yousef, the mastermind behind the 1994 World Trade Center bombing and 1995 bombing of a Manila Air airliner, encrypted files stored on his laptop computer. When authorities seized his computer in Manila and decrypted the files, they found information pertaining to further plans to blow up 11 U.S.-owned commercial airliners in the Far East.[84]

There have been several terrorist incidents involving physical attacks against computers and telecommunications systems. In the 1970s, for example, the Italian Red Brigades launched 27 attacks against businesses in the electronics, computer, and weapons industries.[85] Their manifesto specified the destruction of computer systems and installations as a way of "striking at the heart of the state. "[86]

Software attacks against computer systems of a destructive nature are sometimes characterized as "information terrorism." These include computer penetrations that sabotage and delete computer files, intentionally releasing a computer virus onto a network, and Internet-based attacks that disrupt service and shut down computers remotely. For the most part, however, these activities have not been conducted by terrorists in the traditional sense but by hackers and disgruntled employees. They have been aimed at a particular organization, not an entire country, and their impact has been limited mainly to the organizations attacked. Their objective has not been to cause physical violence.

In what some u.s. intelligence authorities characterized as the first known attack by terrorists against a country's computer systems, ethnic Tamil guerrillas were said to have swamped Sri Lankan embassies with thousands of electronic mail messages. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications."87 An offshoot of the Liberation Tigers of Tamil Eelam, which have been fighting for an independent homeland for minority Tamils, was responsible for the incident.88

The e-mail bombing consisted of about 800 e-mails a day for about two weeks. William Church, editor for the Centre for Infrastructural Warfare stud- ies (CIWARS), observed that "the Liberation Tigers of Tamil are desperate for publicity and they got exactly what they wanted. ..considering the routinely deadly attacks committed by the Tigers, if this type of activity distracts them from bombing and killing then CIWARS would like to encourage them, in the name of peace, to do more of this type of' terrorist' activity."89 The attack, how- ever, had the desired effect of generating fear in the embassies. It also could be the forerunner of more destructive attacks against computers on the Internet.

In the 1980s, Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term "cyberterrorism" to refer to the convergence of cyberspace and terrorism.9° IvIark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer pro- grams, and data which result in violence against noncombatant targets by subnational groups or clandestine agents." 91

Is cyberterrorism the way of the future? For a terrorist, it would have some advantages over physical methods. It could be conducted remotely, it would be cheap, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, as journalists and the public alike are fascinated by practically any kind of computer attack. One highly acclaimed study of the risks of computer systems began with a paragraph that

concludes "Tomorrow's terrorist may be able to do more with a keyboard than with a bomb." 92

In a 1997 paper, Collin describes several possible scenarios. In one, a cyber- terrorist hacks into the processing control system of a cereal manufacturer and changes the levels of iron supplement. A nation of children get sick and die. In another, the cyberterrorist attacks the next generation of air traffic control systems. Two large civilian aircraft collide. In a third, the cyberterrorist disrupts banks, international financial transactions, and stock exchanges. Economic systems grind to a halt, the public loses confidence, and destabilization is achieved.93

Analyzing the plausibility of Collin's hypothetical attacks, Pollitt concludes that there is sufficient human involvement in the control processes used today that cyberterrorism does not-at present-pose a significant risk in the classical sense. In the cereal contamination scenario, for example, he argues that the quantity of iron (or any other nutritious substance) that would be required to become toxic is so large that assembly line workers would notice. They would run out of iron on the assembly line and the product would taste different and not good. In the air traffic control scenario, humans in the loop would notice the problems and take corrective action. Pilots, he says, are trained to be aware of the situation, to catch errors made by air traffic controllers, and to operate in the absence of any air traffic control at all.94

Pollitt does not imply by his analysis that computers ate safe and free from vulnerability. To the contrary, his argument is that despite these vulnerabilities, because humans are in the loop, a cyber attack is unlikely to have such devastating consequences. He concludes that " As we build more and more technology into our civilization, v\Te must ensure that there is sufficient human oversight and intervention to safeguard those whom technology serves. At least two independent studies have suggested that financial systems are vulnerable to an information warfare attack by terrorists or other hostile parties. One, by Tom Manzi, argues that the Clearing House Interbank Payment System (CHIPS) or the Fedwire funds transfer system operated by the Federal Reserve System could be knocked out for an extended period of time by a physical attack that uses a combination of car bombs and electromagnetic weapons.95 Another, by Air Force Cadet Edward Browne, argues that the systems are well protected physically but that CHIPS is vulnerable to an attack that exploits the daily lag of credits against debits.96 Brian S. Bigelow, a major in the U.S. Air Force, dismisses both scenarios, arguing that they do not hold water when tested against the real conditions in the financial industry. Like Pollitt, Bigelow argues that there are substantial checks and balances in these systems. "Both Browne's and Manzi's scenarios illustrate the suspension of disbelief that undermines the credibility of many infowar discussions. The use of computers and networks undeniably creates vulnerabilities, but to say this makes them the Achilles' heel of the financial services infrastructure is to ignore the very considerable measures institutions have taken to manage their information systems risks."97

Telecommunications systems have suffered numerous outages but so far none that induced more than temporary hardship. The May 1998 satellite out- age illustrates. When the PanAmSat Corp. satellite spun out of control on Tuesday evening, May 19, it crippled most u.s. paging services as well as some data and media feed. The company immediately began shifting signals onto other PanAmSat satellites, while doctors, nurses, and police officers switched to alter- native technologies such as walkie-talkies, portable radios, and cellular telephone,~. National Public Radio began distributing *All Things Considered* via phone lines and a RealAudio feed on its Web site. By Thursday morning, 75% of businesses that depended on the satellite had been assigned alternative bandwidth. PageNet, the largest pager service in the country, said 85% of their 10.4 million customers had working beepers by Thursday and that the rest were expected to be operational by Friday. According to the *Washington Times,* "no one was re- ported seriously injured by the satellite's failure. There were no howls from Wall Street about lost deals." 98

In an article titled "How Many Terrorists Fit on a Computer Keyboard?" William Church presents a strong case that the United States does not yet face a compelling threat from terrorists using information warfare techniques to dis- rupt critical infrastructure. They lack either the motivation, capabilities, or skills to pull off a cyber attack at this time. Church does not rule out a physical attack against the infrastructure, but such a threat is neither new nor matured by U.S. reliance on technology.99 In another essay, Church includes terrorists in his list of information warfare threats against the United States. In decreasing priority, the threats are organized crime (financial fraud and extortion), individual hacker terrorism, politically oriented nongovernment organizations, physically violent terrorist groups, and finally other states. 100 Clark Staten testified that it was believed that "members of some Islamic extremist organizations have been at - tempting to develop a 'hacker network' to support their computer activities and even engage in offensive information warfare attacks in the future." 10l

Early indicators suggest that terrorist groups may use the Internet more to influence public perception and coordinate their activities than to launch highly destructive and disruptive attacks, at least against the Net itself. The Internet is likely to have greater value to them when it is fully operational. If that is the case, then it will also be in their interest to keep the supporting infrastructures running, including those for telecommunications and power .

At least for the time being, the terrorist threat from bombs and weapons of mass destruction, particularly chemical and biological weapons, may be greater than from cyber at tacks. 102 The effects are likely to be more violent and have a greater psychological impact than anything that can be accomplished in

cyberspace. Further, there is more uncertainty associated with cyber attacks. It is easier to predict the damages from a well-placed bomb than from shutting down computer systems, releasing a virus, or tampering with electronic files. So far, the most destructive attacks have been perpetrated by hackers fooling around or protesting policies and by persons seeking revenge against their former employers. None of these have caused fatalities.

Cyber attacks may be used as an ancillary tool in support of other operations-just as they may support, but not replace, more conventional military operations. To illustrate, in early 1998, a design flaw was reported in a security badge system used widely in airports, state prisons, financial institutions, military contractors, government agencies (including the CIA), and high-tech companies. The vulnerability would have allowed an intruder to use a dial-up line or network connection to create permanent or temporary badges for gaining access to secured areas, unlock doors guarding sensitive areas, schedule events such as unlocking all doors at a particular time, and create badges that left no record of a person entering and leaving a secured area.1O3 One can imagine a terrorist group attempting to exploit such a vulnerability as part of a larger operation to penetrate airport security. That done, explosives might be hidden on board an aircraft.

None of this is to say that a catastrophic cyber attack cannot and will not occur .The future cannot be predicted, and an attack might proceed in ways that have not been anticipated. Thus, it is worth taking steps to ensure that critical infrastructures are sufficiently hardened to defeat an adversary, whether a terrorist, foreign government, hacker, or high-tech thief. It is also worth constructing scenarios such as those postulated by Collin, Manzi, Browne, and others as they offer a powerful tool for discovering and analyzing potential vulnerabilities and threats.

Netwars

At the same time they introduced the concept of cyberwar to think about military operations conducted according to information-related principles, Arquilla and Ronfeldt introduced "netwar" to think about information-related struggles most often associated with low-intensity conflict by nonstate actors, including nongovernment organizations (NGOs) .They predict that future conflicts will be fought by groups that are organized more as networks than as hierarchies. They argue that networks can defeat institutions and that hierarchies have a difficult time fighting networks. They are particularly interested in "all-channel networks," in which every node can communicate with every other node. This type of network is a natural outgrowth of modern technologies, particularly the Inter- net, which offer easy connectivity between any two entities. Arquilla and Ronfeldt believe the network form to be one of the most significant effects of the

information revolution for all realms: political, economic, social, and military. Power is migrating to those who can readily organize as sprawling networks. "The future may belong to whoever masters the network form." 104 As in cyberwar, a variety of technical and nontechnical weapons will be employed in netwar. Operations will attempt to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it. They will involve psyops and perception management, including public diplomacy measures, propaganda, political and cultural subversion, deception of or interference with local media, and efforts to promote dissident or opposition movements across computer networks. Netwars will exploit information technologies and may involve infiltration of computer networks. They can be waged between the governments of rival nation-states; by governments against illicit groups such as those involved in terrorism, drugs, or proliferation of weapons of mass destruction; or by political advocacy groups against governments. An example of netwar can be found in the struggle between the Zapatista National Liberation Army (EZLN) and the government of Mexico. On New Year's Day 1994, EZLN insurgents occupied six towns in Chiapas, declared war on the Mexican government, demanded changes, and initiated a global media campaign. They issued press releases, invited foreigners to come to Chiapas and observe the situation for themselves, and sponsored conferences. They sought political, economic, and social reforms, including rights for indigenous people, legitimate and fair elections, repeal of 1992 provisions governing land tenure, and a true political democracy. The Mexican army reclaimed the territory, but the Zapatistas endeavored to compensate for their lack of physical power by dominating the information space. 105 The Zapatistas and their supporters have used the Internet to spread word about their situation and to coordinate activities. One group of New York sup- porters, the Electronic Disturbance Theater (EDT), organized an attack against Mexican President Zedillo's Web site. On April 10, 1998, participants in the at- tack pointed their Web browsers to a site with FloodNet software, which bombarded the target site with traffic (see also Chapter 8). The EDT planned to repeat the attack on May 10 but changed their plans when the Mexican-based human rights group AME LA PAZ (LOVE PEACE) protested. The group objected to any type of attack that would violate the law: "It is clear that there is a war in Internet the Zapatistas are wining [sic] ...But this war, and this is what is important, has been won within the boundaries of the law. ...The EZLN does not suggest or want the civil society supporting them to take unlawful actions." In response, EDT revised their plans, attacking President Clinton's White House Web site in- stead.106 Even then, the Zapatistas distanced themselves from the attack. On September 9, EDT once again struck the Web site of President Zedillo, along with those of the Pentagon and the Frankfurt Stock Exchange. The Net strike was launched in conjunction with the Ars Electronica Festival on Infowar, held in Liz, Austria. According to Brett Stalbaum, author of the FloodNet software used in the attack, the Pentagon was chosen because "we believe that the U.S. military trained the soldiers carrying out the human rights abuses." Stalbaum said the Frankfurt Stock Exchange was selected because it represented globalization, which was at the root of the Chiapas' problems. EDT estimated that up to 10,000 people participated in the demonstration, delivering 600,000 hits per minute to each of the three sites. The Web servers operated by the Pentagon and Mexican government, however, struck back. When they sensed an attack from the FloodNet servers, they opened window after window in the users' browsers, in some cases forcing the protestors to reboot their computers. The Frankfurt Stock Exchange reported that they normally get 6 million hits a day and that services appeared unaffected. 107

This example adds further support to the notion that the Internet may prove more valuable as a means of influencing public opinion and coordinating activity than as a target of destructive operations. Individual nodes on the Inter- net may be attacked, but doing so requires that the infrastructure itself remain intact.

Protecting National Infrastructures

The U.S. government has taken several steps to defend national information infrastructures. Although it is beyond the scope of this book to cover all of them, two are particularly noteworthy and referenced in later chapters. The first was the formation of a Computer Emergency Response Team Coordination Center (CERT */CC)* at Carnegie- Mellon University. CERT */CC* was established in 1988 following a major incident on the Internet that disrupted thousands of computers (see the Internet Worm in Chapter 10). The Department of Defense Advanced Research Projects Agency, which founded the Internet, created the CERT */CC* so that the United States would be better prepared for future incidents. CERT /CC was to offer a 24-hour point of contact and a central point for identifying vulnerabilities and working with the vendor community to resolve them.

Since the creation of CERT, numerous other incident-handling and response centers have been created within the federal government, including the Department of Energy's Computer Incident Advisory Capability (CIAC) and the Defense Information Systems Agency's ASSIST. In 1989, the Forum of Incident Response and Security Teams (FIRST) was established to facilitate information exchange and coordination among these centers. These efforts led to the formation of a Federal Computer Incident Response Center (FedCIRC), which pro- vides a government-wide incident response capability on a subscription basis.lo8

The second was the formation of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996. The PCCIP was asked to study

the critical infrastructures that constitute the life support systems of the nation, determine their vulnerabilities to a wide range of threats, and propose a strategy for protecting them in the future. Eight infrastructures were identified: telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services. In their final report, issued in October 1997, the commission reported that the threats to critical infrastructures were real and that, through mutual dependence and interconnectedness, they could be vulnerable in new ways. "Intentional exploitation of these new vulnerabilities could have severe consequences for our economy, security, and way of life."

The PCCIP noted that cyber threats have changed the landscape. "In the past we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports. Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be in- visibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker."109

In assessing the threat from both physical and cyber attacks, the PCCIP concluded that "Physical means to exploit physical vulnerabilities probably re- main the most worrisome threat to our infrastructures *today.* But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyber threats *before* they materialize and produce major sys- tem damage." 110 The recommendations of the PCCIP are summarized in the last chapter of this book along with follow-on initiatives, including the establishment of the National Infrastructure Protection Center (NIPC) and Presidential Decision Directive (PDD) 63.

That critical systems are potentially vulnerable to cyber attacks was under- scored by a June 1997 exercise, code named Eligible Receiver, conducted by the National Security Agency (NSA). The objective was to determine the vulnerability of U.S. military computers and some civilian infrastructures to a cyber at- tack. According to reports, two- man teams targeted specific pieces of the military infrastructure, including the U.S. Pacific Command in Hawaii, which oversees 100,000 troops in Asia. One person played the role of the attacker, while another observed the activity to ensure that it was conducted as scripted. Using only readily available hacking tools that could easily be obtained from the Internet, the NSA hackers successfully gained privileged access on numerous systems. They concluded that the military infrastructure could be disrupted and possible troop deployments hindered. The exercise also included written scenarios against the power grid and emergency 911 systems, with resulting service disruptions. For the latter, they postulated that by sending sufficient e-mails to Internet users telling them the 911 system had a problem, enough curious people would phone 911 at once to overload the system. No actual attacks were made against any civilian infrastructures.