Photo © Tony Stone Images / Stephen Johnson

A Presidential commission warns that we may not even know when we're under attack.

War in Cyberspace

By John T. Correll, Editor in Chief

LAST winter, a flood of some 30,000 messages swamped the e-mail system at Langley AFB, Va., the headquarters of Air Combat Command. They virtually shut the system down for several hours until network administrators devised programs to filter out the disruptions. As investigators reconstructed it later, the messages originated in Australia and Estonia and were routed through several intermediate points, including the White House computer system. The perpetrators have not been identified.

That may have been a small-scale preview of how an enemy of the future might choose to launch a strike, rather than challenging US military superiority head-on.

"While once an attack on our nation's infrastructures had to overcome physical distance and physical borders, now an adversary can gain access to the heart of our infrastructures from anywhere instantaneously and can use that instant access to do harm," said Robert T. Marsh, chairman of the President's Commission on Critical Infrastructure Protection, which spent 15 months studying the nation's vulnerability to electronic attack.

There are perhaps 20 million people who have the means and skill to do some level of damage. It requires no more than a 486 computer and a modem. The software, instructions, and targeting information can be gotten from hacker sites on the Internet.

The threats to the public and private sectors overlap. For example, most military communications are now carried by commercial channels. "National defense is not just about government anymore, and economic security is not just about business," the Marsh commission said in its report to the President in October.

■ In 1992, a refinery in California could not use its emergency alert network to notify the surrounding area of an accidental release of toxic substances because a disgruntled employee had accessed the data system and disabled the warning mechanism for more than 25 sites.

■ In 1996, a hacker, using an electronic service denial technique that had been written up in two hacker magazines, bombarded the system of an Internet service provider in New York and practically shut down access for 6,000 individuals and nearly a thousand corporate subscribers for a week.

■ In 1997, malicious calls from a Swedish hacker jammed the 911 emergency telephone lines in Miami, disrupted service, harassed the operators, and diverted 911 calls hither and yon. He also accessed a telephone system and generated 60,000 unauthorized calls. He was tried as a juvenile in Sweden and fined the equivalent of $345.

Electronic Pearl Harbor

The Marsh commission was established in July 1996 amid concerns that, as former Sen. Sam Nunn put it, the nation might be headed for an "electronic Pearl Harbor." Nunn said, for example, that Department of Defense information systems were coming under attack about 250,000 times a year and that more than half of those attempts had been successful. The number of attacks is increasing and is now believed to approach 500,000 a year.

The commission was chartered to examine the threats to eight critical national infrastructures: information and communications, electrical power systems, transportation, oil and gas delivery and storage, banking and finance, emergency services, water supply systems, and government services. However, what the commission found was that the problem centers on the information and communications sector—the public telecommunications network, the Internet, and the millions of computers in home, government, and commercial use.

"Our security, economy, way of life, and perhaps even survival are now dependent on the interrelated trio of electrical energy, communications, and computers," said Marsh, a retired Air Force four-star general and a former commander of Air Force Systems Command.

The commission arrayed the threats on three levels. So far, most of the activity has been at the lowest level and are "local threats," which include recreational hackers, vandals, and independent thieves. At the next level are "shared threats" from institutional hackers, organized crime, and industrial espionage. The ultimate concern is "national threats," which encompass full-up information warfare and attacks by foreign governments or terrorists.

"Today, a computer can cause switches or valves to open and close, move funds from one account to another, or convey a military order almost as quickly over thousands of miles as it can from next door, and just as easily from a terrorist hideout as from an office cubicle or military command center," the commission report said. "A false or malicious computer message can traverse multiple national borders, leaping from jurisdiction to jurisdiction to avoid identification, complicate lawful pursuit, or escape retribution."

A complicating factor is that only about 17 percent of the attacks on communications and data networks are reported to law enforcement authorities. The commission report said that victims "expressed reluctance to share information about vulnerabilities, fearing it might be made public, resulting in damage to their reputations, exposing them to liability, or weakening their competitive position. Many also feared that sharing vulnerability information could invite unwanted federal regulation."

Another complication is that the problem is not widely recognized. Several industry decision makers told the commission that "there has not yet been a cause for concern sufficient to demand action."

Big, Vulnerable Networks

The number of computers in the United States has risen from 5,000 in 1960 to about 180 million today. More than 95 percent of these are personal computers.

Over the past 15 years, many of these machines have been linked into a vast network through public telephone lines and the Internet, "creating an extended information and communications infrastructure that has changed the way we live and work," the commission report said. "This infrastructure has swiftly become essential to every aspect of the nation's business, including national and international commerce, civil government, and military operations."

The transformation continues. "Current trends suggest that the public telecommunications network and the Internet will merge in the years ahead; by 2010, many of today's networks will likely be absorbed or replaced by a successor public telecommunications infrastructure capable of providing integrated voice, data, video, private line, and Internet-based services," the commission said.

This trend leads not only to greater economy and convenience but also to new and greater vulnerabilities.

In times past, the telephone company sent out somebody in a truck to hook up service or check out problems. Today, much of the network maintenance is performed through remote access. Services ranging from cable television to the Internet are also managed to large degree by remote electronic access.

"The channels used for remote access by authorized maintenance personnel offer potential attack routes for adversaries," the Marsh

How the Hackers Attack

Eight of the 10 founders of WheelGroup in San Antonio are former members of the Air Force Information Warfare Center. Their team—named after the computer slang term for UNIX group zero (the "wheel"), which controls the network—is now among the nation's leaders in electronic security. Last year, in a demonstration organized by *Fortune* magazine and with the consent of the targeted firm, WheelGroup operators penetrated the well-defended computer networks of a Fortune 500 company in New York. Their methods illustrate some of the ways in which hackers attack.

They began their attack via the Internet, "bouncing" an e-mail with a deliberate error in it to gain pathway information from the returned message. They then "pinged" all of the computer ports at the target firm to see if any were open. However, the firm had invested in a good (and expensive) "fire wall," and rather than spend time trying to break through, WheelGroup went directly after the company's computer modems instead.

Beginning with an employee's business card and figuring that most of the target telephone numbers would have the same area code and three-digit prefix, WheelGroup "war-dialed" 1,500 numbers, using a program downloaded from the Internet.

Several of the numbers responded. One, a fax server at a subsidiary, invited WheelGroup to "log in," which it did, moving deeper and deeper into the network from there. Another modem offered WheelGroup a "C" prompt, the same kind that is familiar to millions of personal computer users. Playing a guess, WheelGroup typed in "Win," and—sure enough—was rewarded with a Microsoft Windows program screen and from there, a welcome to the corporate tax department, where all manner of information and records were stored. WheelGroup gained "root access" in short order and, true to its name, was in position to control the networks it had targeted.

Fortune quoted *E-mail Security* author Bruce Schneier, who says that "the only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location—and I'm not completely confident of that one either."

commission said. "Once logged on, an attacker can remove nodes from service and disrupt the network."

It is difficult to distinguish between an electronic attack and the accidental failure of a network. In June 1991, service for 6.7 million telephone lines in Washington, D.C., was disrupted for several hours. The problem turned out to be a mistake in the telephone switching protocol—a single mistyped character of code. An attack on the telephone system might take much the same form.

Furthermore, the commission report said, "The tools designed to access, manipulate, and manage the information or communications components that control critical infrastructures can also be used to do harm. They are inexpensive, readily available, and easy to use."

We do not even have the capability to know when we're under attack. "Deciding whether a set of cyber and physical events is coincidence, criminal activity, or a coordinated attack is not a trivial problem," the commission report said. "Without a central repository and analytic capability, it is virtually impossible to make such assessments until after the fact."

Administrators on the Ramparts

The defenses consist mainly of scattered security practices, virus scanners, passwords, and "fire walls." Few organizations have specialized electronic security people. "Our first line of protection is with the system administrators and computer people," said Phillip E. Lacombe, the commission's staff director.

Those working the problem say they are laboring with inadequate tools, information, and coordination of effort. They must also operate within a legal system that never envisioned an attack on the nation's telecommunications switches from a distant computer keyboard.

"Looping and weaving" is standard operating procedure for accomplished hackers. They route their attack through a series of computers, which may be located in several different countries. Security people have the technical ability to "hack back" the signal to its source, but at present, they're allowed to track it only to the last computer in the series. Going further requires a court order for every computer in the chain. On the security shopping list, therefore, is a national "trap and trace" law in which a single court order would allow pursuit all the way back to the hacker.

(Doug Richardson, writing in *Armada International*, says the Air Force has devised methods to damage computers used in hacker attacks and has destroyed expendable 486 computers in demonstration tests.)

Other provisions of the law make people in the private sector wary of sharing information, revealing problems, or cooperating with the federal government. For example, the Freedom of Information Act makes information in the possession of the government available to the public. Private sector participants want better assurances than are available now that sensitive information or trade secrets will remain confidential.

In particular, the private sector is cautious on the issue of encryption, the scrambling of data so that it cannot be decoded without a key. Initially, the Clinton Administration had opposed strong encryption systems, especially if they might be exported, unless federal law enforcement and intelligence officials were given the means to unscramble the encryption.

Getting almost no acceptance of that notion, the Administration now seeks a compromise solution—which is endorsed by the Marsh commission—that would have the deciphering keys held by trusted third parties. The Administration argues that this would permit the same sort of legal protection that currently exists for mail and telephone communications but also ensure court- authorized access for law enforcement officials. That proposal has not generated much enthusiasm from industry, either.

Among the electronic security questions yet to be resolved are: What do we guard against? How do you recognize harmful information? Even if you can recognize it, how and where do you screen for it?

In the case of online cyber attack from abroad, a signal must enter the United States either through a major satellite-downlink site, of which there are just over a dozen, or by way of telecommunications cables, said Lacombe. That might seem to reduce entry points to a manageable number. On the other hand, he added, information might enter as three separate pieces of nonmalicious data that become malicious when they are combined. There are other techniques to evade detection as well.

And of course, if the attacker can arrange to work from a computer located in the United States, a multitude of attack routes will lie open.

A New Partnership

The Marsh commission's budget proposals are modest. At present federal spending on infrastructure protection amounts to only $250 million a year, about $150 million

Global Technology Trends

	in 1982	in 1996	in 2002
Personal computers	thousands	400 million	500 million
Local area networks	thousands	1.3 million	2.5 million
Wide area networks	hundreds	thousands	tens of thousands
Viruses	some	thousands	tens of thousands
Internet devices accessing the World Wide Web	none	32 million	300 million
Population with skills for a cyber attack	thousands	17 million	19 million
Telecommunications systems control software specialists	few	1.1 million	1.3 million

The United States, where nearly half the world's computer capacity (180 million computers out of 400 million) and 60 percent of Internet assets reside, is at once the most advanced and most dependent user of information technology. The last line on the chart shows the population of systems control software specialists who possess the tools and know-how to disrupt or take down the public telecommunications network.

of which is spent on information security. The commission recommended doubling the amount to $500 million a year. Much of that is for research and development of real-time detection, identification, and response tools and for means to prevent attack, mitigate damage, recover service, and reconstitute architectures.

What the commission proposed mainly is the creation of a new partnership between government and the private sector and the establishment of a national point of focus.

"National security is a shared responsibility," Marsh said. "The private sector is responsible for taking prudent measures to protect itself from commonplace hacker tools. If these tools are also used by the terrorist, then the private sector will also be protecting itself from cyber terrorist attack and will be playing a significant role in national security.

"The federal government is responsible for collecting information about the tools, the perpetrators, and their intent from all sources, including the owners and operators of the infrastructures. The government must then share this information with the private sector so that industry can take the necessary protective measures."

The commission called for an Office of National Infrastructure Assurance within the White House, reporting to the National Security Council and serving as the federal government's focal point for infrastructure protection.

A number of other organizations were proposed as well, notably "clearinghouses" as focal points for industry cooperation and sharing. Clearinghouses might be operated by associations or trade groups.

How the partnership would operate where national security is concerned is even less clear. It has not been determined when or whether a cyber attack would constitute an act of war or what the nation would do about it if it occurred.

If such an attack is an act of war, the Department of Defense would have major if not sole responsibility for response. It is not presently organized to meet such a responsibility.

In a speech in September, Marsh made passing reference to "a recent Joint Staff exercise" in which "some of the issues were quite troubling—including the fact that the Joint Staff ended up fighting this war, which was not only bad but illegal."

He was talking about Joint exercise "Eligible Receiver," an element of which was an adversary using cyber tools. Public law vests the war making powers of the United States in the hands of the National Command Authorities and the commanders of the unified combat commands. This part of the exercise did not fit the mission of any of the unified commanders, so in the simulation, the Joint Staff took charge itself, which it could not legally do in an actual conflict.

The Marsh commission also proposed one or more federal agencies to coordinate work on each of the critical infrastructures. The Treasury Department would be lead agency for banking and finance matters, for example, and the Department of Energy for electrical power vulnerabilities.

Federal responsibility for the pivotal information and communications sector would be shared by the Departments of Defense and Commerce. Inevitably, the Justice Department would be involved as well. In the view of Attorney General Janet Reno, who has been active on the infrastructure protection problem from the beginning, the same sort of relationship that developed between the Departments of State and Defense during the Cold War now needs to develop between Justice and Defense.

Given the ambiguity of electronic threats, the Marsh commission concluded that "initially, all cyber attacks will have to be treated as crimes—regardless of where they originated or the purpose of the attack. When investigation provides evidence of foreign government involvement or the magnitude of the attack requires it, then other leadership may be assigned." ▪

The Datastream Cowboy and Kuji

The best known of all attacks on Air Force data systems began on March 23, 1994, with penetration of the Rome Laboratory computer network at Rome, N.Y. Five days had passed before Rome discovered that the attack was under way, and before it ended 26 days later, 150 known intrusions had taken place. The hackers gained complete access to 30 systems, downloaded data, and used Rome as a launching platform to penetrate about 100 other systems, including computers at NASA, the Jet Propulsion Laboratory in Pasadena, Calif., and the Goddard Space Flight Center in Greenbelt, Md.

Using a variety of techniques, investigators learned that there were two hackers, using the handles "Datastream Cowboy" and "Kuji." They also discovered early that the final links in the attack chain were Internet service providers in New York and Seattle.

April 15 was a tense day. The hackers used the Rome computers to tap and download information from the Korean Atomic Research Institute. At first, the Air Force was fearful that the institute might be in North Korea and an intrusion from Rome Lab might be perceived by the suspicious North Koreans as an act of war. As it turned out, the institute was in South Korea.

The Air Force Office of Special Investigations got a lead on the Datastream Cowboy through his indiscretion in declaring his handle in an e-mail exchange with another hacker. He said he lived in the United Kingdom and that he liked to attack "dot mil" sites, or military computers. Unknown to Datastream, the hacker on the other end of the e-mail exchange was an OSI informant.

New Scotland Yard began monitoring Datastream's telephone in London. Instances of "phone phreaking" from his number—manipulating British Telecom to zero out billing records and thus make calls free—coincided with intrusions at Rome Lab. He routed his attacks, variously, through South America, Europe, Mexico, and Hawaii.

Datastream was arrested in May 1994. According to the *Times* of London, when the police came for him, he "curled up on the floor and cried." His name was Richard Pryce and he was 16 years old. He was using a 25 mHz, 486 SX desktop computer with a 170 megabyte hard drive at a workstation on the third floor of his family's home. On March 21, 1997, Datastream was sentenced in Bow Street Magistrates Court in London, for 12 counts of hacking in violation of the Computer Misuse Act. He was fined a total of £1,200 plus £250 court costs.

Kuji, several years older than Datastream, was not arrested until June 1996. He was revealed to be Matthew James Bevan, a computer technician from Cardiff in Wales. He has been charged under a tougher section of the Computer Misuse Act than Datastream was. At present, he is free on bail and reporting on his own case from his site on the World Wide Web.