FOCUS

THE BOSTON SUNDAY GLOBE • MARCH 5, 1995

TECHNOLOGY

The Manchurian printer

What if they gave a war .... and it was fought by modem?

In "The Manchurian Candidate," Angela Lansbury uses her son, Laurence Harvey, as the secret tool of a foreign power. Tomorrow's equivalent weapons may be high tech rather than human.

BY SIMSON L. GARFINKEL

Early last month, Hewlett Packard announced a recall of 10,000 HP OfficeJet printer fax copiers. The printer's power supplies may have a manufacturing defect that could pose an electrical shock hazard. HP says that it discovered the problem during routine testing. HP was lucky: Printers can be very dangerous devices. A typical laser printer, for example, can draw hundreds of watts of power, generate internal temperatures high enough to burn a wayward human hand and, under the right circumstances, even start a fire.

Most manufacturers, of course, try to design their printers to minimize such risks. Increasingly, however, there is a chance that companies might intentionally design life-threatening flaws into their products so that the flaws can be exploited later. These fatal flaws might be intentionally built into equipment manufactured overseas, as a kind of "insurance policy" in the event of a war between that country and the United States. The flaws might form the basis for a new kind of corporate warfare. Or they might be hidden by disgruntled employees contemplating extortion or revenge.

Indeed, US military planners are increasingly worried about this sort of possibility, which they place under the heading "Information Warfare." Nevertheless, although the threat of information warfare is very real, an even bigger danger is that the Defense Department will use this threat to persuade the new Congress to repeal the Computer Security Act of 1987. This would effectively allow the National Security Agency to declare martial law in cyberspace and could send the civilian computer industry into a tailspin.

To understand what the military is afraid of, imagine what one might call "the Manchurian Printer": a low-cost, high-quality laser printer, manufactured overseas, with a built-in, secret self-destruct sequence. For years these printers could lie dormant. But send them a special coded message – perhaps a long sequence of words that would never normally be printed together – and the printer would lock its motors, overheat and burst into flames. Such an attack might be the first salvo in an out-and-out war between the United States and the country's manufacturer. Alternatively, an enemy company might simply use printers to start selective fires, damage economic competitors, take out key personnel and cause mischief.

The technology behind the Manchurian Printer isn't science fiction. In October, Adobe Systems accidentally shipped a "time bomb" in its Photoshop version 3.0 for the Macintosh. A time bomb is a little piece of code buried inside a computer program that makes the software stop running after a particular date. Adobe put two time bombs into its Photoshop 3.0 program while the application was under development. The purpose behind the time bombs was to force anybody who got an advance, pre-release copy of the program to upgrade to the final shipping version. But when it came time to ship the final version, Adobe's engineers made a mistake: They took out only one of the bombs.

An engineer at Adobe learned about the problem soon after the product was shipped, and the company quickly issued a recall and a press release. Adobe called the time bomb a "security code time constraint" and said that "although this is an inconvenience to users, the security constraint neither damages the program or hard drive, nor does it destroy any files."

It only takes a touch of creativity and a bit of paranoia to think up some truly malicious variants on this theme. Imagine that a company wants to make a hit with its new word processor: Instead of selling the program, the company gives away free evaluation copies that are good for one month. What's unknown to the users of this program is that while they are typing in their letters, the program is simultaneously sniffing out and booby-trapping every copy of Microsoft Word and WordPerfect that it finds on your system. At the end of the month, all your word processors stop working: Instead of letting you edit your memos, they print out ransom notes.

Any device that is equipped with a microprocessor can be equipped with such a booby trap. Radios, cellular telephones and computers that are connected to networks are particularly vulnerable, since an attacker can send them messages without the knowledge or consent of their owners. Some booby traps aren't even intentional. What makes them particularly insidious is that it is almost impossible to look at a device and figure out if one is present or not. And there is no practical way to test for them, either. Even if you could try a million combinations a second, it would take more than 200 years to find a sequence that was just 8 characters long.

Information warfare isn't limited only to things that break or go boom. The Defense Department is also worried about security holes that allow attackers to break into commercial computers sitting on the Internet or take over the telephone system.

"This nation is under IW attack today by a spectrum of adversaries ranging from the teen-age hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems," says a report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield, issued in October by the secretary of defense.

"Information Warfare could pervade throughout the spectrum of conflict to create unprecedented effects. Further, with the dependence of modern commerce and the military on computer-controlled telecommunication networks, data bases, enabling software and computers, the US must protect these assets relating to their vulnerabilities," the report warns.

Information warfare changes the rules of fighting, the report says. A single soldier can wreak havoc on an enemy by reprogramming the opposing side's computers. Modern networks can spread computer viruses faster than missiles carrying biological warfare agents – and conceivably do more damage. Worst of all, the tools of the information warrior are readily available to civilians, terrorists and uniformed soldiers alike, and we are all potential targets.

Not surprisingly, the unclassified version of the Pentagon's report barely mentions the offensive possibilities of information warfare – capabilities that the Pentagon currently has under development. Nevertheless, these capabilities are alluded to in several of the diagrams, which show a keen interest by the military in OOTW – Operations Other Than War.

"They have things like information influence, perception management and PSYOPS – psychological operations," says Wayne Madsen, a scientist at the Computer Sciences Corp. in northern Virginia, who has studied the report. "Basically, I think that what they are talking about is having the capability to censor and put out propaganda on the networks. That includes global news networks like CNN and BBC, your information services, like CompuServe and Prodigy," and communications satellite networks. "When they talk about 'technology blockade,' they want to be able to block data going into or out of a certain region of the world that they may be attacking."

The report also hints at the possibility of lethal information warfare – meaning, Madsen says, "screwing up navigation systems so airplanes crash and ships runs aground. Pretty dangerous stuff. We could have a lot of Iranian Airbuses crashing if they start screwing that up," he says. Indeed, according to Madsen, the Army's signal warfare center in Warrenton, Va., has already invited companies to develop computer viruses for battlefield operations.

Our best defense against information warfare is designing computers and communications systems that are fundamentally more secure. Currently, the federal organization with the most experience in the field of computer security is the National Security Agency, the world's foremost spy organization. But right now, NSA's actions are restricted by the 1987 Computer Security Act, which forbids the agency from playing a role in the design of civilian computer systems. As a result, one of the implicit conclusions of the Pentagon's report is to repeal the 1987 law and so untie the NSA's hands. Indeed, the Pentagon is now embarking on a high-level campaign to convince lawmakers that such a repeal would be in the nation's best interests.

This argument confuses security with secrecy. It also ignores the reasons the Computer Security Act was passed in the first place.

In the years before 1987, the NSA was on a campaign to expand its power throughout society by using its expertise in the field of computer security as a lever. The NSA tried to create a new category of restricted technical information called "national security related information." They asked Mead Data Corp. and other literature-search systems for lists of their users with foreign-sounding names. And, says David Banisar, a policy analyst with the Washington-based Electronic Privacy Information Center, "they investigated the computers that were used for the tallying of the 1984 presidential election. Just the fact that the military is looking in on how an election is being done is a very chilling thought. After all, that is the hallmark of a banana republic."

The Computer Security Act was designed to nip this in the bud. It said that standards for computer systems should be set in the open by the National Institute of Standards and Technology.

Unfortunately, the Clinton administration has found a way to get around the law. It's placed an "NSA liaison officer" four doors down from the NIST director's office. The two most important civilian computer standards to be designed in recent years – the nation's new Escrowed Encryption Standard (the "Clipper" chip) and the Digital Signature Standard – both were designed in secret by the NSA. The NSA also has been an unseen hand behind the efforts on the part of the Clinton administration to make the nation's telephone system "wiretap friendly."

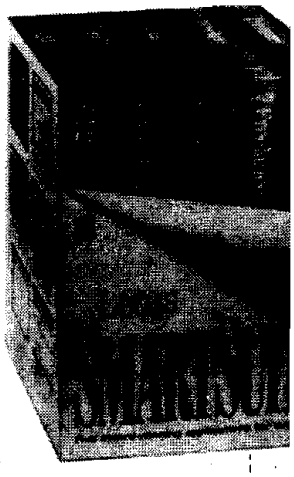
Many computer scientists have said the NSA is designing weak standards that it can circumvent, so that the nation's information warfare defenses do not get in the way of the agency's offensive capability. Unfortunately, there's no way to tell for sure. That's the real problem with designing security standards in secret: There is simply no public accountability.

In this age of exploding laser printers, computer viruses and information warfare, we will increasingly rely on strong computer security to protect our way of life. Just as important, these standards must be accountable to the public. We simply can't take our digital locks and keys from a Pentagon agency that's saying "trust me." But the biggest danger of all would be for Congress to simply trust the administration's information warriors and grant their wishes without any public debate.

Simson L. Garfinkel is a contributing writer for Wired magazine.

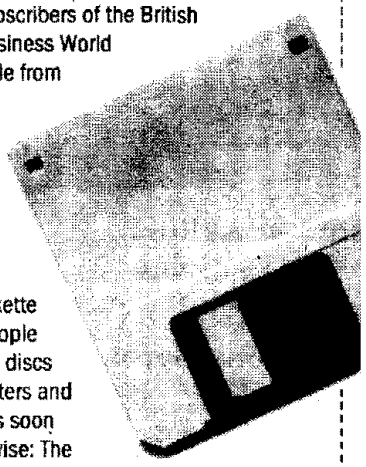
■ Is your cellular phone turned on? Then your phone is broadcasting your position every time it sends out its electronic "heartbeat." Some law enforcement agencies now have equipment that lets them home in on any cellular telephone they wish (similar technology was used recently to catch infamous computer criminal Kevin Mitnick). Perhaps that's the reason the Israeli government recently ordered its soldiers along the border to stop using their cellular telephones to order late-night pizzas: The telephone's radio signal could become a homing beacon for terrorist missiles.

Smart bombs (of a sort)

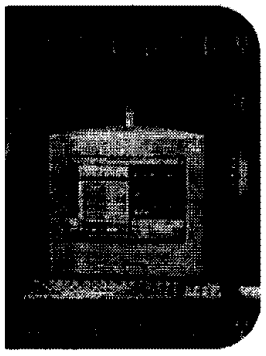


■ Even though it's illegal, a lot of people like to "try out" software by making a copy of a friend's before they plunk down their own hundreds of dollars. Computer companies say this is a form of software piracy: Many who try never buy. More than $2 billion in software is pirated annually, according to the Business Software Alliance.

One way that companies such as Microsoft and Lotus could fight back is by booby-trapping their software. Sure, customers wouldn't like it if that stolen copy of Microsoft Word suddenly decided to erase every letter or memo they've written in the past month, but what legal recourse would they have?



■ Beware of discs bearing gifts. In 1989, nearly 7,000 subscribers of the British magazine PC Business World and 3,500 people from the World Health Organization's database received a disc in the mail labeled "AIDS Information Introductory Diskette Version 2.0." People who inserted the discs into their computers and ran the programs soon found out otherwise: The discs actually contained a so-called "Trojan horse" that disabled the victims' computers and demanded a ransom.



■ Several years ago, users of Prodigy were shocked to find that copies of documents on their computers had been copied into special "buffers" used by Prodigy's DOS software. Prodigy insisted that the copied data were the result of a software bug and it wasn't spying on its customers. But if you use a modem to access America Online, Prodigy or CompuServe, there is fundamentally no way to be sure that your computer isn't spying on you while you surf the information highway.