ISSUES IN SCIENCE AND TECHNOLOGY online

Fall 1998



How Vulnerable is our Interlinked Infrastructure?

George Smith

# An Electronic Pearl Harbor? Not Likely

**The government's evidence about U.S. vulnerability to cyber attack is shaky at best.Information warfare: The term conjures up a vision of unseen enemies, armed only with laptop personal computers connected to the global computer network, launching untraceable electronic attacks against the United States. Blackouts occur nationwide, the digital information that constitutes the national treasury is looted electronically, telephones stop ringing, and emergency services become unresponsive.**

But is such an electronic Pearl Harbor possible? Although the media are full of scary-sounding stories about violated military Web sites and broken security on public and corporate networks, the menacing scenarios have remained just that-only scenarios. Information warfare may be, for many, the hip topic of the moment, but a factually solid knowledge of it remains elusive.

**Hoaxes and myths about information warfare contaminate everything from official reports to newspaper stories.**

There are a number of reasons why this is so. The private sector will not disclose much information about any potential vulnerabilities, even confidentially to the government. The Pentagon and other government agencies maintain that a problem exists but say that the information is too sensitive to be disclosed. Meanwhile, most of the people who know something about the subject are on the government payroll or in the business of selling computer security devices and in no position to serve as objective sources.

There may indeed be a problem. But the only basis on which we have to judge that at the moment is the sketchy information that the government has thus far provided. An examination of that evidence casts a great deal of doubt on the claims.

**Computer-age ghost stories**

Hoaxes and myths about info-war and computer security-the modern equivalent of ghost stories-contaminate everything from newspaper stories to official reports. Media accounts are so distorted or error-ridden that they are useless as a barometer of the problem. The result has been predictable: confusion over what is real and what is not.

A fairly common example of the type of misinformation that circulates on the topic is illustrated by an article published in the December 1996 issue of the FBI's *Law & Enforcement Bulletin*. Entitled "Computer Crime: An Emerging Challenge for Law Enforcement," the piece was written by academics from Michigan State and Wichita State Universities. Written as an introduction to computer crime and the psychology of hackers, the article presented a number of computer viruses as examples of digital vandals' tools.

A virus called "Clinton," wrote the authors, "is designed to infect programs, but . . . eradicates itself when it cannot decide which program to infect." Both the authors and the FBI were embarrassed to be informed later that there was no such virus as "Clinton." It was a joke, as were all the other examples of viruses cited in the article. They had all been originally published in an April Fool's Day column of a computer magazine.

The FBI article was a condensed version of a longer scholarly paper presented by the authors at a meeting of the Academy of Criminal Justice Sciences in Las Vegas in 1996. Entitled "Trends and Experiences in Computer-Related Crime: Findings from a National Study," the paper told of a government dragnet in which federal agents arrested a dangerously successful gang of hackers. "The hackers reportedly broke into a NASA computer responsible for controlling the Hubble telescope and are also known to have rerouted telephone calls from the White House to Marcel Marceau University, a miming institute," wrote the authors of their findings. This anecdote, too, was a rather obvious April Fool's joke that the authors had unwittingly taken seriously.

The FBI eventually recognized the errors in its journal and performed a half-hearted edit of the paper posted on its Web site. Nevertheless, the damage was done. The FBI magazine had already been sent to 55,000 law enforcement professionals, some of them decisionmakers and policy analysts. Because the article was written for those new to the subject, it is reasonable to assume that it was taken very seriously by those who read it.

Hoaxes about computer viruses have propagated much more successfully than the real things. The myths reach into every corner of modern computing society, and no one is immune. Even those we take to be authoritative on the subject can be unreliable. In 1997, members of a government commission headed by Sen. Daniel Moynihan (D-N.Y.), which included former directors of the Central Intelligence Agency and the National Reconnaissance Office, were surprised to find that a hoax had contaminated a chapter addressing computer security in their report on reducing government secrecy. "One company whose officials met with the Commission warned its employees against reading an e-mail entitled Penpal Greetings," the Moynihan Commission report stated. "Although the message appeared to be a friendly letter, it contained a virus that could infect the hard drive and destroy all data present. The virus was self-replicating, which meant that once the message was read, it would automatically forward itself to any e-mail address stored in the recipient's in-box."

Penpal Greetings and dozens of other nonexistent variations on the same theme are believed to be real to such an extent that many computer security experts and antivirus software developers find themselves spending more time defusing the hoaxes than educating people about the real thing. In the case of Penpal, these are the facts: A computer virus is a very small program designed to spread by attaching itself to other bits of executable program code, which act as hosts for it. The host code can be office applications, utility programs, games, or special documents created by Microsoft Word that contain embedded computer instructions called macro commands-but not standard text electronic mail. For Penpal to be real would require *all* electronic mail to contain executable code automatically run when someone opens an e-mail message. Penpal could not have done what was claimed.

That said, there is still plenty of opportunity for malicious meddling, and because of it, thousands of destructive computer viruses have been written for the PC by bored teenagers, college students, computer science undergraduates, and disgruntled programmers during the past decade. It does not take a great leap of logic to realize that the popular myths such as Penpal have contributed to the sense, often mentioned by those writing about information warfare, that viruses can be used as weapons of mass destruction.

**The widely publicized figure of 250,000 hacker intrusions on Pentagon computers in 1995 is fanciful.**

Virus writers have been avidly thinking about this mythical capability for years, and many viruses have been written with malicious intent. None have shown any utility as weapons. Most attempts to make viruses for use as directed weapons fail for easily understandable reasons. First, it is almost impossible for even the most expert virus writer to anticipate the sheer complexity and heterogeneity of systems the virus will encounter. Second, simple human error is always present. It is an unpleasant fact of life that all software, no matter how well-behaved, harbors errors often unnoticed by its authors. Computer viruses are no exception. They usually contain errors, frequently such spectacular ones that they barely function at all.

Of course, it is still possible to posit a small team of dedicated professionals employed by a military organization that could achieve far more success than some alienated teen hackers. But assembling such a team would not be easy. Even though it's not that difficult for those with basic programming skills to write malicious software, writing a really sophisticated computer virus requires some intimate knowledge of the operating system it is written to work within and the hardware it will be expected to encounter. Those facts narrow the field of potential professional virus designers considerably.

Next, our virus-writing team leader would have to come to grips with the reality, if he's working in the free world, that the pay for productive work in the private sector is a lot more attractive than anything he can offer. Motivation-in terms of remuneration, professional satisfaction, and the recognition that one is actually making something other people can use-would be a big problem for any virus-writing effort attempting to operate in a professional or military setting. Another factor our virus developer would need to consider is that there are no schools turning out information technology professionals who have been trained in virus writing. It's not a course one can take at an engineering school. Everyone must learn this dubious art from scratch.

And computer viruses come with a feature that is anathema to a military mind. In an era of smart bombs, computer viruses are hardly precision-guided munitions. Those that spread do so unpredictably and are as likely to infect the computers of friends and allies as enemies. With militaries around the world using commercial off-the-shelf technology, there simply is no haven safe from potential blow-back by one's creation. What can infect your enemy can infect you. In addition, any military commander envisioning the use of computer viruses would have to plan for a reaction by the international antivirus industry, which is well positioned after years of development to provide an antidote to any emerging computer virus.

To be successful, computer viruses must be able to spread unnoticeably. Those that do have payloads that go off with a bang or cause poor performance on an infected system get noticed and immediately eliminated. Our virus-writing pros would have to spend a lot of time on intelligence, gaining intimate knowledge of the targeted systems and the ways in which they are used, so their viruses could be written to be maximally compatible. To get that kind of information, the team would need an insider or insiders. With insiders, computer viruses become irrelevant. They're too much work for too little potential gain. In such a situation, it becomes far easier and far more final to have the inside agent use a hammer on the network server at an inopportune moment.

But what if, with all the caveats attached, computer viruses were still deployed as weapons in a future war? The answer might be, "So what?" Computer viruses are already blamed, wrongly, for many of the mysterious software conflicts, inexplicable system crashes, and losses of data and operability that make up the general background noise of modern personal computing. In such a world, if someone launched a few extra computer viruses into the mix, it’s quite likely that no one would notice.

**Hackers as nuisances**

What about the direct effects of system-hacking intruders? To examine this issue, it is worth examining in detail one series of intrusions by two young British men at the Air Force’s Rome Labs in Rome, New York, in 1994. This break-in became the centerpiece of a U.S. General Accounting Office (GAO) report on network intrusions at the Department of Defense (DOD) and was much discussed during congressional hearings on hacker break-ins the same year. The ramifications of the Rome break-ins are still being felt in 1998.

One of the men, Richard Pryce, was originally noticed on Rome computers on March 28, 1994, when personnel discovered a program called a "sniffer" he had placed on one of the Air Force systems to capture passwords and user log-ins to the network. A team of computer scientists was promptly sent to Rome to investigate and trace those responsible. They soon found that Pryce had a partner named Matthew Bevan.

Since the monitoring was of limited value in determining the whereabouts of Pryce and Bevan, investigators resorted to questioning informants they found on the Net. They sought hacker groupies, usually other young men wishing to be associated with those more skilled at hacking and even more eager to brag about their associations. Gossip from one of these Net stoolies revealed that Pryce was a 16-year-old hacker from Britain who ran a home-based bulletin board system; its telephone number was given to the Air Force. Air Force investigators subsequently contacted New Scotland Yard, which found out where Pryce lived.

By mid-April 1994, Air Force investigators had agreed that the intruders would be allowed to continue so their comings and goings could be used as a learning experience. On April 14, Bevan logged on to the Goddard Space Center in Greenbelt, Maryland, from a system in Latvia and copied data from it to the Baltic country. According to one Air Force report, the worst was assumed: Someone in an eastern European country was making a grab for sensitive information. The connection was broken. As it turned out, the Latvian computer was just another system that the British hackers were using as a stepping stone.

On May 12, not long after Pryce had penetrated a system in South Korea and copied material off a facility called the Korean Atomic Research Institute to an Air Force computer in Rome, British authorities finally arrested him. Pryce admitted to the Air Force break-ins as well as others. He was charged with 12 separate offenses under the British Computer Misuse Act. Eventually he pleaded guilty to minor charges in connection with the break-ins and was fined 1,200 English pounds. Bevan was arrested in 1996 after information on him was recovered from Pryce's computer. In late 1997, he walked out of a south London Crown Court when English prosecutors conceded it wasn't worth trying him on the basis of evidence submitted by the Air Force. He was deemed no threat to national computer security.

Pryce and Bevan had accomplished very little on their joyride through the Internet. Although they had made it into congressional hearings and been the object of much worried editorializing in the mainstream press, they had nothing to show for it except legal bills, some fines, and a reputation for shady behavior. Like the subculture of virus writers, they were little more than time-wasting petty nuisances.

But could a team of dedicated computer saboteurs accomplish more? Could such a team plant misinformation or contaminate a logistical database so that operations dependent on information supplied by the system would be adversely influenced? Maybe, maybe not. Again, as in the case of the writing of malicious software for a targeted computer system, a limiting factor not often discussed is knowledge about the system they are attacking. With little or no inside knowledge, the answer is no. The saboteurs would find themselves in the position of Pryce and Bevan, joyriding through a system they know little about.

Altering a database or issuing reports and commands that would withstand harsh scrutiny of an invaded system's users without raising eyebrows requires intelligence that can only be supplied by an insider. An inside agent nullifies the need for a remote computer saboteur or information warrior. He can disrupt the system himself.

The implications of the Pryce/Bevan experience, however, were not lost on Air Force computer scientists. What was valuable about the Rome intrusions is that they forced those sent to stop the hackers into dealing with technical issues very quickly. As a result, Air Force Information Warfare Center computer scientists were able to develop a complete set of software tools to handle such intrusions. And although little of this was discussed in the media or in congressional meetings, the software and techniques developed gave the Air Force the capability of conducting real-time perimeter defense on its Internet sites should it choose to do so.

The computer scientists involved eventually left the military for the private sector and took their software, now dubbed NetRanger, with them. As a company called WheelGroup, bought earlier this year by Cisco Systems, they sell NetRanger and Net security services to DOD clients.

**Inflated numbers**

A less beneficial product of the incidents at Rome Labs was the circulation of a figure that has been used as an indicator of computer break-ins at DOD since 1996. The figure, furnished by the Defense Information Systems Agency (DISA) and published in the GAO report on the Rome Labs case, quoted a figure of 250,000 hacker intrusions into DOD computers in 1995. Taken at face value, this would seem to be a very alarming figure, suggesting that Pentagon computers are under almost continuous assault by malefactors. As such, it has shown up literally hundreds of times since then in magazines, newspapers, and reports.

But the figure is not and has never been a real number. It is a guess, based on a much smaller number of recorded intrusions in 1995. And the smaller number is usually never mentioned when the alarming figure is cited. At a recent Pentagon press conference, DOD spokesman Kenneth H. Bacon acknowledged that the DISA figure was an estimate and that DISA received reports of about 500 actual incidents in 1995. Because DISA believed that only 0.2 percent of all intrusions are reported, it multiplied its figure by 500 and came up with 250,000.

Kevin Ziese, the computer scientist who led the Rome Labs investigation, called the figure bogus in a January 1998 interview with Time Inc's. *Netly News*. Ziese said that the original DISA figure was inflated by instances of legitimate user screwups and unexplained but harmless probes sent to DOD computers by use of an Internet command known as "finger," a check used by some Net users to return the name and occasionally additional minor information that can sometimes include a work address and telephone number of a specific user at another Internet address. But since 1995, the figure has been continually misrepresented as a solid metric of intrusions on U.S. military networks and has been very successful in selling the point that the nation's computers are vulnerable to attack.

In late February 1998, Deputy Secretary of Defense John Hamre made news when he announced that DOD appeared to be under a cyber attack. Although a great deal of publicity was generated by the announcement, when the dust cleared the intrusions were no more serious than the Rome Labs break-ins in 1994. Once again it was two teenagers, this time from northern California, who had been successful at a handful of nuisance penetrations. In the period between when the media focused on the affair and the FBI began its investigation, the teens strutted and bragged for *Anti-Online*, an Internet-based hacker fanzine, exaggerating their abilities for journalists.

Not everyone was impressed. Ziese dismissed the hackers as "ankle-biters" in the *Wall Street Journal*. Another computer security analyst, quoted in the same article, called them the virtual equivalent of a "kid walking into the Pentagon cafeteria."

Why, then, had there been such an uproar? Part of the explanation lies in DOD's apparently short institutional memory. Attempts to interview Hamre or a DOD subordinate in June 1998 to discuss and contrast the differences between the Rome incidents in 1994 and the more recent intrusions were turned down. Why? Astonishingly, it was simply because no current top DOD official currently dealing with the issue had been serving in that same position in 1994, according to a Pentagon spokesperson.

**Info-war myths**

Another example of the jump from alarming scenario to done deal was presented in the National Security Agency (NSA) exercise known as "Eligible Receiver." As a war game designed to simulate vulnerability to electronic attack, one phase of it posited that an Internet message claiming that the 911 system had failed had been mailed to as many people as possible. The NSA information warriors took for granted that everyone reading it would immediately panic and call 911, causing a nationwide overload and system crash. It's a naïve assumption that ignores a number of rather obvious realities, each capable of derailing it. First, a true nationwide problem with the 911 system would be more likely to be reported on TV than the on Internet, which penetrates far fewer households. Second, many Internet users, already familiar with an assortment of Internet hoaxes and mean-spirited practical jokes, would not be fooled and would take their own steps to debunk it. Finally, a significant portion of U.S. inner-city populations reliant on 911 service are not hooked to the Internet and cannot be reached by e-mail spoofs. Nevertheless, "It can probably be done, this sort of an attack, by a handful of folks working together," claimed one NSA representative in the Atlanta *Constitution*. As far as info-war scenarios went, it was bogus.

However, with regard to other specific methods employed in "Eligible Receiver," the Pentagon has remained vague. In a speech in Aspen, Colorado, in late July 1998, the Pentagon's Hamre said of "Eligible Receiver:" "A year ago, concerned for this, the department undertook the first systematic exercise to determine the nation's vulnerability and the department's vulnerability to cyber war. And it was startling, frankly. We got about 30, 35 folks who became the attackers, the red team . . . We didn't really let them take down the power system in the country, but we made them prove that they knew how to do it."

**The time and effort spent dreaming up scary info-war scenarios would be better spent bolstering basic computer security.**

The Pentagon has consistently refused to provide substantive proof, other than its say-so, that such a feat is possible, claiming that it must protect sensitive information. The Pentagon's stance is in stark contrast to the wide-open discussions of computer security vulnerabilities that reign on the Internet. On the Net, even the most obscure flaws in computer operating system software are immediately thrust into the public domain, where they are debated, tested, almost instantly distributed from hacker Web sites, and exposed to sophisticated academic scrutiny. Until DOD becomes more open, claims such as those presented by "Eligible Receiver" must be treated with a high degree of skepticism.

In the same vein, computer viruses and software used by hackers are not weapons of mass destruction. It is overreaching for the Pentagon to classify such things with nuclear weapons and nerve gas. They can't reduce cities to cinders. Insisting on classifying them as such suggests that the countless American teenagers who offer viruses and hacker tools on the Web are terrorists on a par with Hezbollah, a ludicrous assumption.

### Seeking objectivity

Another reason to be skeptical of the warnings about information warfare is that those who are most alarmed are often the people who will benefit from government spending to combat the threat. A primary author of a January 1997 Defense Science Board report on information warfare, which recommended an immediate $580-million investment in private sector R&D for hardware and software to implement computer security, was Duane Andrews, executive vice president of SAIC, a computer security vendor and supplier of information warfare consulting services.

Assessments of the threats to the nation's computer security should not be furnished by the same firms and vendors who supply hardware, software, and consulting services to counter the "threat" to the government and the military. Instead, a true independent group should be set up to provide such assessments and evaluate the claims of computer security software and hardware vendors selling to the government and corporate America. The group must not be staffed by those who have financial ties to computer security firms. The staff must be compensated adequately so that it is not cherry-picked by the computer security industry. It must not be a secret group and its assessments, evaluations, and war game results should not be classified.

Although there have been steps taken in this direction by the National Institute of Standards and Technology, a handful of other military agencies, and some independent academic groups, they are still not enough. The NSA also performs such an evaluative function, but its mandate for secrecy and classification too often means that its findings are inaccessible to those who need them or, even worse, useless because NSA members are not free to discuss them in detail.

### Bolstering computer security

The time and effort expended on dreaming up potentially catastrophic information warfare scenarios could be better spent implementing consistent and widespread policies and practices in basic computer security. Although computer security is the problem of everyone who works with computers, it is still practiced half-heartedly throughout much of the military, the government, and corporate America. If organizations don't intend to be serious about security, they simply should not be hooking their computers to the Internet. DOD in particular would be better served if it stopped wasting time trying to develop offensive info-war capabilities and put more effort into basic computer security practices.

It is far from proven that the country is at the mercy of possible devastating computerized attacks. On the other hand, even the small number of examples of malicious behavior examined here demonstrate that computer security issues in our increasingly technological world will be of primary concern well into the foreseeable future. These two statements are not mutually exclusive, and policymakers must be skeptical of the Chicken Littles, the unsupported claim pushing a product, and the hoaxes and electronic ghost stories of our time.

---

George Smith edits *The Crypt Newsletter,* an Internet publication based in Pasadena, California, dealing with issues related to computer crime, computer security, and information warfare. He is the author of *The Virus Creation Labs: A Journey into the Underground* (American Eagle, 1994), a book analyzing the culture of computer virus writers, the distribution of malicious software, and the rise of the antivirus industry. He can be e-mailed at **crypt@sun.soci.niu.edu**
.

## *Recommended reading*

Computer Underground Digest (http://www.soci.niu.edu/~cudigest) and RISKS Journal (http://catless.ncl.uk/Risks/VL.IS.html). Both are longstanding Internet publications devoted to subjects discussed in this article.

*Critical Foundations: Protecting America's Infrastructure*, report of the President's Commission on Critical Infrastructure Protection (the Marsh Commission Report) (available at http://www.pccip.gov).

The Federation of American Scientists' Information Warfare on the Web clearinghouse (http://www.fas.org/irp/wwwinfo.html).

Clifford Stoll, *Silicon Snake Oil: Second Thoughts on the Information Highway*. New York: Doubleday, 1995.

Virus Myths: A comprehensive Web site devoted to documenting and analyzing techno-myths as they relate to computer viruses, computer security, and information warfare (http://www.kumite.com/myths).