# GHOSTS IN THE MACHINES?

***By Dr. Martin Libicki***
***Senior Policy Analyst, RAND***

*The author cites law enforcement as a primary area where global information security can be enhanced. He calls for "the harmonization of national laws against computer attack, multinational cooperation in tracing attacks across national lines, international treaties on extradition of attackers, and a readiness to impose sanctions on those who protect attackers." He believes a willingness to share information on research and development, on attack indications and warnings, and on attack incidents and responses "can also improve the efficacy of each nation's protective measures."*

No one looking for something new to worry about need look very far. Everywhere, computers and other digital devices have insinuated themselves into our lives. What was manual is now automated; what was analog is now digital; and what once stood alone is now connected to everything else. Increasingly, we have no choice but to trust them. If they fail, we are sunk.

The faith that dependence breeds would be merited if such devices did only what they were supposed to do. Some do fail on their own, and we go on. But the prospect also exists that they may fail us because they have fallen under the control of those with malign intent. In such circumstances, they may not only go down, but reveal secrets with which they have been entrusted, or produce corrupted information — sometimes in ways beyond notice until it is too late to reverse actions already set in motion.

Why the vulnerability? Digital devices are fast, cheap, accurate, and rarely forget what they are told. But they are frightfully literal and usually lack the discernment to understand the implications of what they are asked to do or the integrity of those who ask them to do it.

The potential consequences of deliberately induced systems failure or corruption are vast. By seizing control of the key systems that undergird society, computer attackers can, in theory, listen to phone calls, misroute connections, and stop phone service entirely; shut down electrical power; get in the way of literally trillions of dollars that change hands every week; hinder emergency services; prevent the U.S. military from responding to crises abroad quickly; reveal personal medical secrets; confuse transportation systems and put travelers at risk; and much more. Life, as we know it, could grind to a halt.

Computer attacks, if sufficiently systematic, may be war by other means — hence "information warfare," as an overarching concept. But information warfare understood broadly — attacking an adversary's information and decision processes — is as old as warfare itself. Such tactics encompass psychological operations, attacks on an enemy's command apparatus, espionage and counter-espionage, and operations against adversary infrastructures and surveillance systems. During the U.S. Civil War (1861-1865) there were incidents of propaganda operations, snipers targeting opposing generals and observers in hot-air balloons, marauders tearing up telegraph lines, cavalry pickets and counter-cavalry demonstrations — all information warfare. World War II saw the advent of electronic warfare in the form of radar, electronic deception, radio-frequency jamming, codemaking, and computer-aided codebreaking.

Computer attacks fit snugly into this continuum of warfare. If one can destroy enemy headquarters with shot and shell, what is wrong with trying less violent means to break into and ruin the computer systems that manage tomorrow's battles? Notions of strategic warfare by 1920 held that using air power against civilian targets would short-circuit the gore of trench warfare. Strategic information warfare goes this one better.

Are modern societies vulnerable? Most information systems have far less security than they could have; many, less than they should have. Networks and systems of many types have been attacked — Internet service, phone service, some transport services, financial institutions, and corporate networks.

Computer attacks are, by any indication, a serious problem. Indeed, the Federal Bureau of Investigation recently estimated that they cost the American economy somewhere between a half a billion and five billion dollars a year — an estimate with a wide, and, in its way, very telling, margin of error. No one really knows how many attacks take place. Much evidence is anecdotal, and so people have to extrapolate using popular precepts such as, "only amateurs leave fingerprints, professionals never do," and, "people never want to talk about how badly they have been hit." Thus are computer attacks likened to icebergs, with America, supposedly, playing Titanic.

This is the theory, at any rate. But is it a prospect? Unlike virtually all other forms of warfare, there is no forced entry in cyberspace. If hackers enter a system they invariably have done so along paths resident in the system itself: some are features and some are bugs (that is, undocumented features) never removed. Either way, travel along these paths is under the complete control of whoever is running the system. This being so, vigilance suffices for protection.

Indeed, protections exist. Many information systems operate with several layers: there are ways to screen illegitimate from legitimate users, locks to keep legitimate users from taking deliberate or inadvertent control of computer systems, and safety devices so that even the usurpation of control does not create a public hazard.

Attackers, for their part, must first fool a system into thinking they are legitimate users (e.g., by stealing or guessing a password), and second, acquire control privileges (often by exploiting endemic faults) denied to most common users. With such "super-user" privileges, attackers can purge key files, write errant nonsense in others, or plant a backdoor for later reentry.

There is also little doubt that defenses, if need be, could be better than today's common practice.

Most systems use passwords to limit entry, but passwords have many well-known problems: too many are easy to guess; they can be stolen as they flow over networks, and they are too commonly stored in expected places on a server. Cryptographic methods such as digital signatures work around these problems (capturing and replaying access messages does not work). Digital signatures even help ensure that any change to a data base or program, once electronically signed, can be traced to its originator — also useful, if the attacker is an insider entrusted with systems privileges.

Computer and network operating systems are susceptible to hacker-inserted programs such as viruses (software that infects software and causes it to infect other software), Trojan horses (seemingly useful software with hidden traps), and logic bombs (software that lies dormant until signalled). Virus-protection programs may work, but if worries persist, why not put all the critical files on an unalterable medium (e.g., a CD-ROM)? Such a medium can also prevent information from being erased or corrupted by a would-be attacker's digital footprints. Indeed, given the low cost of such devices, there is no legitimate excuse for losing information anymore.

Systems can also be put at risk from other systems they hold to be trustworthy. Two precautions can be taken against this danger: culling the list of trustworthy systems and limiting the number of messages that one's own system will react to. Banking systems, for instance, do this to protect their computers from being corrupted by ATMs (automatic teller machines) sitting on a public street corner. The computer ignores anything from the ATM that is not a legitimate transaction. No legitimate transaction can wreck the bank computer.

A final precaution is to pull the plug. As a last resort, many systems (e.g., nuclear power plants) work almost as well even if unconnected to the outside world.

How far must a system's owners go? Relatively low-cost security protection (e.g., firewalls and intrusion detectors) may seem good enough for the current environment. After all, an office system may not be worth spending great sums of money to protect if, for example, an attack will only disrupt service temporarily. Many companies perceive no serious threat and invest accordingly. They may be right — but what if they are wrong? If and as threats mount, systems owners can increase security — even in the short run (e.g., by preventing users from logging in from home, or carrying out certain actions if logged on).

Indeed, it is precisely the lack of good security features throughout the national information infrastructure today that leads to some confidence that computer systems could, if necessary, be made safe. (By contrast, good defenses against nuclear warfare were technologically impossible for decades, and, if possible today, are very costly.) Even if many systems can be taken down temporarily, it is another matter to keep them down for a long time while systems administrators work fiendishly to restore essential services. Anyone who would hold the U.S. information infrastructure at risk must realize that the mere threat of doing so — if taken seriously — erodes soon after being announced as people react.

What should the role of government be? Can those responsible for protecting the nation on the ground, on the water, in the air, and in outer space also protect the nation in cyberspace? Should they?

Government can help, but there is much government cannot do — or should not do. Yes, electricity is essential, but protecting its supply from hackers depends almost entirely on how power companies manage their computer systems: this includes the network and operating system software they buy, how such software is configured, how access privileges are awarded and protected, and how the various fail-safe and manual override mechanisms are emplaced throughout the companies' generation and distribution systems. It is inconceivable that any power company would wish the government to "protect" it by telling it how to do these things. More generally, the government cannot build a firewall around the United States — if only because so many internal networks span the globe.

The government can and does enforce laws against computer attacks — and has experienced considerable success considering how anonymous (and faraway) attackers can be. So far, most of the well-publicized hacker attacks that have been detected have been the work of amateurs not professionals.

Should the government try to inhibit information warfare by threatening retaliation against perpetrators? Assume their identity can be established. The U.S. government may threaten like for like, but many rogue states have little in the way of comparable systems (e.g., North Korea lacks a stock market to take down). Conversely, it is problematic to respond violently to an information warfare attack that wasted the victim's time and money, but wounded no one.

While much of what the government can do to enhance security is indirect, the President's Commission on Critical Infrastructure Protection and other entities have made the following recommendations:

— Make sure the government's own systems are protected, because they are important to national security and for setting a standard for others.

— Use research, development, and first-user acquisition to promote the rapid development of security tools.

— Disseminate warnings of impending information warfare attacks (if they can be detected — no small task).

— Promote a legal framework that induces private parties to protect their own systems to the optimal extent.

— Provide a neutral clearinghouse that encourages private parties to collaborate on sharing their experiences and countermeasures on a confidential basis.

By and large, such measures are progressing.

Unfortunately, U.S. government restrictions, extant and threatened, on hard encryption have inhibited one of the better tools for protecting systems and also have reduced the credibility of government actions in the information warfare area.

International Activities: Extending most of these government actions overseas suggests an opening agenda for guiding international activities against information warfare.

Law enforcement is a big area. The harmonization of national laws against computer attack, multinational cooperation in tracing attacks across national lines, international treaties on extradition of attackers, and a readiness to impose sanctions on those who protect attackers can all aid global information security.

A readiness to share information on research and development, on attack indications and warnings, as well as attack incidents and responses can also improve the efficacy of each nation's protective measures. However these areas are often the province of intelligence agencies, not historically noted for transparency in such matters.

Conclusions and Harbingers: In the post-Cold War world, there is an increase in new and unconventional threats (e.g., nuclear-armed terrorists) which are scary, but, as yet, notional. Information warfare is among them. The more that information systems pervade society — its defenses, commerce, and day-to-day life — the more their well-being matters to us all. The potential for major mischief does exist, particularly if undertaken in a systematic way by a well-financed adversary. But what is also striking is the fact that even though information warfare is relatively inexpensive, so far, there has been a paucity of really damaging incidents.

Two indicators may reveal a great deal about the true risk from systems attack. One is how people react to the year 2000 computer problem. Assume a large share of the world's information systems crash at midnight on December 31, 1999. Will panic and paralysis result, or will people quickly find ways of working around the problem or doing without information for awhile? If lawsuits erupt, what precedents will be established to assign responsibility to people for harm done if their systems fail?

The other harbinger is of more recent origin. Were one to imagine the most plausible perpetrator of serious information warfare terrorism, it would be someone with nothing that can be held at risk (i.e., not a country), several hundred million dollars in hidden cash, an appreciation of technology, an international network of nefarious friends, and a vicious score (real or imagined) to settle with the United States or some other nation. Sound familiar? If it does, what happens in the next year may reveal whether powerful individuals or groups might try to bring a country to its knees through information warfare — or whether they direct their efforts elsewhere. ◉