Computer Espionage, Titan Rain and China

James A. Lewis

In 1998, computer networks in the Pentagon came under sustained 'attack' for several days. Solemn officials came to the conclusion that China was the attacker and they began to contemplate having the Department of Defense launching some kind of cyber counterstrike when a little more investigation showed that the attacker was not the Peoples Liberation Army but bored teenagers in Cupertino, California.

Cyberwar averted, and a useful lesson to contemplate as we regard the latest round of computer network penetrations at DOD facilities attributed to the Chinese (named "Titan Rain"). First, the Chinese intelligence services are generally not so clumsy as to leave a trail of foot prints leading from the scene of the crime back to China. The goal in an intelligence activity like this is to have 'plausible deniability,' the ability to have your foreign ministry issue a sniffy statement that credibly proclaims innocence. A sophisticated opponent, and China is one of several sophisticated opponents that we face, would launch an attack from a third country. There are many cities around the world where communications facilities are adequate and law enforcement not so energetic.

The internet makes it easy to launch these third country attacks. They are common. China is particularly susceptible to being used as a platform for third country attacks because its networks are so vulnerable. Hackers can take over poorly secured Chinese computers and use them for criminal purposes without their owners' knowledge.

There are several reasons why many Chinese networks are insecure. These include the use of legacy equipment, poor security practices and, perhaps most important, the widespread use of pirated software in China. Some estimates say that up to 90% of the software (such as operating systems) used in China is pirated. It is hard to obtain the patches and security updates for pirated software, and pirated software is sometimes modified to add spyware or other vulnerabilities. The Chinese government knows its networks are vulnerable (annual surveys by the Ministry of Public Safety routinely find more than three quarter of Chinese computers infected with malware) and has created research programs and other incentives to come up with Chinese security software products.

Along with Chinese networks, American universities provide another large pool of vulnerable computers. Universities have large networks with a constantly high level of activity that must be easily accessible to students and faculty. The Cuckoo's Egg, published in 1989 by Cliff Stoll, tells the story of how an Eastern bloc service (probably the KGB) hired a group of West German hackers to steal data from U.S. military computers. The West Germans connected remotely to university networks in the U.S. and used them for the attacks. When the West Germans were finally tracked down and arrested, they did not know who had commissioned them. It is not safe to assume that hostile intelligence services have become less cunning in the years that have intervened.

So an attack that can be traced back to China demonstrates little about the source. China is also the threat du jour. In the 1980s, Americans looked under their beds and believed they saw the KGB; now they believe they see the PLA. A hostile service from a third country might be drawn to use Chinese computers to launch an attack hoping that our proclivity to ascribe bad intent to China would cloud any investigation.

The source of the attack may not even be a hostile intelligence service. Sophisticated hacking tools are widely available on the internet. A skilled virtual community of cybercriminals has grown up in the last few years, trading tools, renting compromised networks and hiring out for attacks. The easily accessible tools give hackers capabilities that were available only to the larger intelligence services a few years ago, and work in the Intelligence community concludes that large multinational corporations could, if they wished, purchase intelligence capabilities as good as or better than those fielded by a medium sized country.

Unlike the bored teenagers of Cupertino, today's hackers include professional criminals whose goal is not excitement but money. These cybercriminals might steal data from the Department of Defense for their own purposes, at the behest of an intelligence service, or even under contract to a business competitor. None of these are imaginary scenarios – Air Force computers were hacked in August 2005 and the personal data of 33,000 Air Force Officers stolen. The goal appears to have been identity theft, not espionage.

China is unlikely to be the source of this set of attacks, but that does not mean that China is not engaged in computer espionage. The Internet is an immense gift to spies. Information that once required physical access or recruitment of agents can now be downloaded from afar. China has a domestic communications intelligence program called "Golden Shield" that uses new technologies to monitor domestic the internet; it is likely that technologies developed for Golden Shield are also used for foreign intelligence collection. China's military is copying the U.S. military and developing 'computer network operations' to attack U.S. information resource and, perhaps, infrastructure in the event of a conflict. Russia, France, Israel and others, even North Korea, have similar programs.

But absent a conflict, the last thing that an intelligence service that had successfully penetrated an opponent's networks would want is to be noticed. The goals are either to get in, collect data, and send it out unobserved or to sit there unobtrusively. In either case, if someone stumbles across the effort, you will want to have covered your tracks well enough that blame cannot be ascribed.

The ease of computer espionage puts a heavy burden on defense. Networks will be vulnerable for a long time. DOD is actually among the less vulnerable agencies. While no classified U.S. network appears to have been compromised, there is an immense quantity of valuable data on open systems, particularly in government research facilities and in the private sector. We should assume that those who want it have already downloaded much of this stored data. But as new information is put online, the U.S. should worry less about who is attacking – assume everyone is attacking – and pay more attention to basic security measures: authenticating users, encrypting data, regular patching, and monitoring systems for intrusions.