Global Information Assurance Certification Paper

The New Front Line
February 20, 2001
J. Wayne Lloyd

"The nature of warfare has changed dramatically. The combatant that wins the information campaign prevails. Information is the key to modern warfare, strategically, operationally, tactically, and technically." *General Glen Otis, former commander of the U.S. Army Training and Doctrine Command.*

Our front lines during a time of war have changed. No longer can we, the United States, rely on the vast bodies of the Atlantic and Pacific oceans to shield us from a war. With the coming of the Internet and the relatively low cost of powerful home personal computers the front line is now located in our place of business, in our homes, and in our nation's most secured facilities. Countries and organizations that have interests that oppose the United States are currently probing and breaking into our nation's critical infrastructure to find vulnerabilities to plant trojans, viruses, and backdoors that will allow them to be incapacitated during a time of crisis.

To give an example of what information warfare could entail, during a time of war an aggressor could use conventional means to attack an ally or a nation in which the United States has a critical interest. At the same time they could employ Information Warfare against our critical infrastructure to slow or stop any response from the United States. This could be accomplished by taking down our electric power grid, which powers our military bases or by disabling commercially owned and computer controlled telephone systems, over which 95% of U.S. military and intelligence communications travel. Financial systems could be disrupted stopping international fund transfers, which could cause the stock market to crash. Banks' computers would start to credit and debit personal accounts at random, which would throw the populace into a panic and cause them to run to withdraw their money. Commercial transportation systems such as air traffic and railway traffic can be affected, causing flights to be delayed or worse, planes to collide. Passenger and freight trains could be derailed or misrouted due to computers not interpreting correct locations of the trains on the tracks. Water treatment plants could be shut down cutting off the water supply to highly populated urban centers in the United States. Damns could be shut down or have their floodgates opened up causing catastrophic flooding, displacing and killing citizens. Oil refineries that are run by computer control could cause explosions and fires.

While all this goes on emergency response entities such as fire and police would be unable to respond effectively if at all. National Guard and Reserve units that would likely have been called upon by the U.S. military to boost manpower during a time of war would now have to be diverted to help flood victims or control rioting because of power blackouts and stock market crashes.

All this could be done without the aggressor ever having to cross their borders or firing a shot at the United States. They would have caused as much damage to the United States' critical infrastructure using computers as if they had used bombs. They would have thrown the nation into a state of panic, and the world's most powerful nation in cyberspace would be brought to its knees by one of its greatest assets -- its technology and its dependence on it.

The above is not a piece of science fiction but a real possibility. China, for example, has formed its own Information Warfare unit. According to Timothy Thomas of the U.S. Army's Foreign Military Studies Office, "China is rapidly integrating the latest state of the art information warfare techniques into its "People's War" strategy. China's new high-tech information warfare capabilities will pose both strategic and operational problems for the West." China has conducted information warfare games that focused on planting information mines, conducting information reconnaissance, changing network data, releasing information bombs, dumping garbage, disseminating propaganda, applying information deception, releasing clone information, organizing info-defense and establishing network spy stations.

In a book by James Adams, "*The Next World War*", he states that "Articles appearing in Chinese military journals talk openly of using doctored chips and software to plant viruses in an enemy's information systems, which would be done by paying off chip producers to make the necessary adjustments." He also brings to light a book written by two Chinese military strategists. The book is titled *America Russia and the Revolution in Military Affairs by PLA officers Zhu Xiaoli and Zhao Xiaozhu*. In it they predict that the gap between China and the United States in information technology dominance will close by the year 2007, at which point America's much vaunted dominance in information technologies will be over, they say, thanks to its own complacency and overconfidence."

Russia has also started its own information warfare unit. The United States Intelligence community has been monitoring computer hackers coming from Russia for over a year. News Max reports, "The hackers are targeting our power plants, telecommunications systems, bridges, damns, sewage treatment plants, water stations and other key installations." Some believe this is proof that Russia is developing its own information warfare techniques.

Middle Eastern groups that have strong feelings against Israel and the United States ties to Israel, strike out at the United States by attacking companies such as Lucent who do business in Israel. Other companies that also do business with Israel have come under attack as well. These attacks are generally in the form of web defacements. Though web defacements show that the system is not as secure as it should be it also could have a much broader affect; it can undermine confidence in the public's eye that that company has secure

systems. This could be devastating to an e-commerce-based company.

Terrorist Osama bin Laden currently employs information warfare against the United States. In this case he uses it to encrypt and cloak his communications over the Internet and within his organizations. Wired News reports "bin Laden allegedly uses encryption -- and a variant of the technology, called steganography -- to evade U.S. efforts to monitor his organization."

Cuba, whose military could not hope to stand up against the United States military in a conventional war, is looking towards another means to attack the United States…Information Warfare. An article from Wired News states, "Admiral Tom Wilson, head of the Defense Intelligence Agency, says the 74-year-old communist dictator may be preparing a cyber attack against the United States." They also wrote "It might seem odd to view a country best known for starving livestock, Elian Gonzalez and acute toilet paper shortages as a looming threat, but the Pentagon seems entirely serious. "

The United States has taken steps to combat aggressors targeting U.S. infrastructure and domestic companies. In May of 1998 the White House announced Presidential Decision Directive (PDD) 63. It sets up a structure to meet the objectives of preventing, deterring, responding to and investigating attacks on the nation's critical infrastructure. It also seeks voluntary participation on the part of private industry to meet common goals for protecting critical systems through public-private partnerships. These goals are to be met by the year 2003.

It is the responsibility of the people who work with, use, and maintain our systems to protect them. System administrators need to install hardened systems before bringing them online to an operational environment. Once installed, they need to be kept up to date with security patches and software updates. System audits are a must. They can help to improve the administrators' understanding of the day-to-day activities of the system, as well as help to find security breaches. Other security measures should be taken such as installing firewalls. (However, firewalls can be gotten around. One way is by taking advantage of a computer system that has a trusted relationship with the organization that has implemented the firewall.) If the system has poor or no security, a hostile user can use it to pass through the firewall) Also malicious code placed in web pages and emails can compromise the security of a firewall since mail and web traffic is allowed to pass through the firewall.

This is where network intrusion detection systems, and anti-virus software should be used to augment the systems security. Good security policies should be written and employees made aware of them, the security policies must also be enforced. In most cases it is not the employee that breaks the security policies of a company but the upper management. Employees that just use their computers for word processing or email need to be educated on the dangers of

social engineering. People posing as admin, helpdesk personnel, or upper management requesting sensitive information such as passwords or changes to user accounts could lead to a compromise of the computer system.

The “I Love You Virus” is an example of social engineering. It played on personal feelings to entice people to open and execute the virus. It is also an example of information warfare. The virus would change registry settings making the web browser go to a specific web page. If the user clicked on a link it would then download a program and gather passwords off of the system. Once the information had been gathered it would then email that information back to the program's author. This was so successful the ISP that hosted the email address thought that it was under a denial of service attack from the flood of incoming email traffic.

With the introduction of board band access via cable modems and DSL to home users the information war is brought into our homes. No longer are we secure behind the front door to our home. To foreign nations as well as malicious hackers, high-speed connections to the internet are prime targets. This is because a vast majority of the connections are going to residential homes in which the owners have absolutely no concept of computer security and these connections are always up. If the computer is turned on then it is connected to the Internet. Also home users do not implement any kind of security measures on their systems because they figure that there is nothing on it that a hacker could want. It may be true, they do not want anything on the computer. However what they want is access to and control of the computer. Once they can control it they will use it to compromise other computers, or to build an army of so called “zombie” computers. With this army they can launch denial of service attacks against another computer or computer network. And where will the attacks look like it came from? It will look as if it came from the home user who was lax in securing their personal computer. Approximately 25% of probes that one government agency receives come from these high-speed connected homes. These probes look to see if there are any known vulnerabilities that can be exploited to allow them to gain access to its systems.

There are products on the market that range from free to a reasonable cost to help home users secure their systems. Zone Alarm or Black Ice defender act as firewalls and allow the home user to monitor what is trying to access their pc’s. Antivirus programs are a must for the home user as well. Symantec and McAfee are two of the most well known antivirus vendors. They provide their software not only to home users, but corporations and U.S. government agencies use them as well for protection against viruses. Home users, just like system administrators, cannot just install these products and expect to remain safe. Home users must also be familiar with what is on their system and how it interacts with their system. Software updates for the programs and operating systems need to be installed, especially security updates.

People who use modems to connect to the Internet should not feel they are not under attack. They are at risk just as much as their broad band counterparts are. Programs called war-dialers can sweep through a range of phone numbers looking for modems that will auto answer. Once a connection is made a computer that uses a modem to connect to the Internet is just as susceptible as a computer that has a broad band connection. Also there are programs that look for computers already connected to the Internet. Once they find a vulnerable one they will compromise it and setup a program that will notify the hacker when that computer is online again so the hacker will not have to go looking for that computer again, it will go looking for them.

As you can see, if and when the United States goes to war again, not only will her men and women in arms be on the front line, but her citizens as well will be combating the enemy in their homes or places of work. If you are connected to the Internet it is not a matter of if you will be probed or attacked, it is just a matter of when.

References:

Adams, James "The next world war" Simon & Schuster, 1998

Denning, Dorothy E. "Information Warfare and Security" ACM press, 1999

LoBaido, Anthony "China's high-tech war games", February 3,2001. URL:
http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=21597
February 20,2001

NewsMax.com "Russian Hackers Hitting U.S. Dams Bridges, Power Plants, Telecommunications" November 1, 2000. URL:
http://www.newsmax.com/archive/print.shtml?a=2000/11/1/24737
February 20,2001

Rand Corporation "Information Warfare: A two Edged Sword" URL:
http://www.rand.org./publications/RRR/RRR.fall95.cyber/infor_war.html
February 8, 2001

Gompert, David C. "Keeping information warfare in Perspective" URL:
http://www.rand.org./publications/RRR/RRR.fall95.cyber/perspective.html
February 8, 2001

Luening, Erich "Lucent says Mideast hackers attacked web site" November 2,2000. URL:
http://news.cnet.com/news/0-1007-200-3368676.html
February 20,2001

Verton, Dan "U.S. May face net-based holy war" November 13,2000. URL

http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47-81_STO53940-,00.html
February 20,2001