CYBERWAR:
Strategic Information Warfare
By Robert K. Hiltbrand
Originally published Spring 1999

INTRODUCATION

Before I begin this discussion, I must add this disclaimer. The research information I have gathered for this paper come from open sources. It is my personal belief that the United States, and in particular the Department of Defense and its related civilian agencies, have some tremendous capabilities that the American public won't ever find out about until a national or international crisis arises. I have attempted to present, through the available unclassified sources, what our national strategic information warfare capabilities are and what some perceived weaknesses in our national information infrastructure. This is just a general discussion of the facts.

The Internet, as we know it today, started out as a program for the Department of Defense in 1969. Back then it was called ARPANET and one of its goals was to link up the computer systems of several universities and colleges that were doing research for the United States Military.

"*Almost 30 years after the US Defense Department created the Internet as a communications system invulnerable even to a nuclear attack, the global web of computer networks is itself now viewed as a national security risk by the Pentagon and other military security chiefs*." (1) Cyberspace soldiers have a finder on the mouse, Business Times, Technology Section November 2, 1997.

The concept of guarding the national infrastructure -- especially its critical components -- against attack is also referred to as cyberwar and in a broader context, as strategic information warfare. (2) Strategic Information Warfare: A New Face of War, Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, 1996 RAND Corporation.

As a result of the rapid growth in information technology, the Department of Defense, like the rest of government and the private sector, has become extremely dependent on automated information systems. To communicate and exchange unclassified information, the Department of Defense relies extensively on a host of commercial carriers and common user networks. This network environment offers the Department of Defense tremendous opportunities for streamlining operations and improving efficiency, but also greatly increases the risks of unauthorized access to information. (3) Report to Congressional Requesters, May 1996, Information Security - Computer Attacks At Department Of Defense Pose Increasing Risks, Government Accounting Office/AIMD-96-84, Defense Information Security (511336).

Several federal civilian and national defense agencies estimate that more than 120 countries around the world have established computer attack capabilities. In addition to this fact, most countries are believed to be planning some degree of information warfare as part of their nation's overall strategy. (4) Cyberspace soldiers have a finder on the mouse, Business Times, Technology Section November 2, 1997.

This means that the United States, in order to maintain its present position as a World leader, must maintain its own Information Warfare strategy.

WHAT IS STRATEGIC INFORMATION WARFARE (IW)?

Strategic Information Warfare is the deliberate sabotage (electronically) of a nation-state's national information infrastructure. This could take the form of crashing the financial markets of a nation. Or it could also be the deliberate shutting down of the power grid in the capital city of an adversary. The worst case scenario could be the infiltration of an enemy's military computer networks with the intent to destroy those very systems and thus prevent those military forces from deploying to the field of battle.

Why is Information Warfare important to the United States? Because we live in a society where computer networks are all around us. Power grids are controlled by complex computer networks. Financial transactions are more and more being conducted electronically. The advent of the Internet. The popularity of email. Air traffic controllers using computer to sort our the traffic in the skies. Any where there is a computer, there is the potential for someone to electronically tamper with the information on it as well as the hardware and equipment it controls. During the American Revolution and the American Civil War, there was armed conflict in the Continental United States. During World War Two, with the attack against Pearl Harbor, more armed conflict was brought to American soil, but not to the Continental United States. But with the advent of Information Warfare, damage can be done directly to the Continental United States without an adversary ever having to physically be near the North American continent. There are no clearly drawn front lines. Anyone and everyone can be affected.

The following quote comes from an American defense analyst, "*Another characteristic of information attacks stems from the loss of sanctuary. Attacks of this sort, particularly when they consist of more than an isolated incident, create a perception of vulnerability, loss of control, and loss of confidence in the ability of the state to provide protection. Thus, the impact can far exceed the actual damage that has occurred. This non-linear relationship between actual damage and societal damage makes the problem of digital war a particularly challenging one because it creates a mismatch between rational defensive responses and their effectiveness.*" (5) Defensive Information Warfare by Dr. David S. Alberts.

As the United States enters the Twenty-first Century with the intention of being a World Leader, we, as a society, must defend our national information infrastructure against attack. Successful attacks against it will have severe, and as yet unknown, economic, political, and societal consequences because of America's heavy reliance upon computer networks. We will discuss America’s vulnerability later.

WHO CAN WAGE INFORMATION WARFARE?

Now that we know what Information Warfare is, the next logical question to ask is, "*Who can wage it*?" Well, the answer is -- anyone. Individual "*hackers*," terrorist organizations with political, economic, or military objectives, or nation-states that would not be able to go head-to-head with a traditional military power such as the United States might be more successful on the cyber battlefield. However, the organizations and nation-states still need the services of the individual hackers to accomplish their goals. We will focus on the hackers because they are the key personnel in offensive Information Warfare. The word "hacker" has many definitions. Webster's New World College Dictionary defines a hacker as a talented amateur of computers, specifically one who attempts to gain unauthorized access to files in various systems. The New Hacker's Dictionary defines a hacker as a person who enjoys exploring the details of programmable systems and how to stretch their capabilities.

A 1996 federal government report about Pentagon computer security states, "*Today the term (hackers) generally refers to unauthorized individuals who attempt to penetrate information systems; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.*" (6) Report to Congressional Requesters, May 1996, Information Security - Computer Attacks At Department Of Defense Pose Increasing Risks, Government Accounting Office/AIMD-96-84, Defense Information Security (511336).

Is a hacker some 14-year-old kid from a Chicago suburb who electronically breaks into his high school's network to change his Home Economics grade from a "*D*" to an "*A*"? How about a group of Russian hackers in St. Petersburg who steal $12 million dollars (US currency) electronically from a Citibank computer located in New York City? (7) Cable News Network news story, March 25, 1999.

George Tenet, Director of the Central Intelligence Agency, had two statements about hackers and their effectiveness in today's globally linked society, "*A group calling themselves the Internet Black Tigers took responsibility for attacks last August (1997) on the e-mail systems of Sri Lankan diplomatic posts around the world, including those in the United States.*" (8) Unclassified Testimony of George J. Tenet, Director of Central Intelligence, delivered to the Senate Committee on Governmental Affairs, June 24, 1998.

"*Italian sympathizers of the Mexican Zapatista rebels crashed web pages belonging to Mexican financial institutions.*" (9) id.

Some of the tools used by individual hackers include -

- Logic bombs - this is unauthorized code that creates havoc when a particular event takes place;
- Virus - code fragment that reproduces by attaching to another program. It can damage hardware and/or software directly, or it can degrade those systems by co-opting resources;
- Trojan horse - independent program that when activated performs unauthorized function (under the guise of doing normal work). Think of it as a nasty little program within a larger normal program.

IS THE UNITED STATES VULNERABLE TO IW ATTACKS?

There are two types of Information Warfare attack modes - structured and unstructured.

An example of an unstructured threat would be how in March, 1997, a 15-year-old Croatian youth hacked his way into the networks at a United States Air Force base in Guam. When questioned about it, the boy just wanted to prove he could do it. (10) Bracing for guerrilla warfare in cyberspace, Cable News Network Interactive by John Christensen, web posted April 6, 1999 @ 1829 Greenwich Mean Time (GMT).

A structured threat would be undertaken by parties that possess intelligence support, proper funding, and are part of their organization or nation-state's long-term strategic goals. (11) Statement of Lieutenant General Kenneth Minihan, United States Air Force and Director of the National Security Agency, to the Senate Governmental Affairs Committee hearing on Vulnerabilities of the national Information Infrastructure, June 24, 1998. An example of a structured attack would be shutting down of the power grid of a City just before it is bombed.

Another statement from General Kenneth Minihan of the NSA, "*The Chinese present a good example of the structured threat. In 1995 the Chinese military openly acknowledged that attacks against financial systems could be a useful asymmetrical weapon.*" (12) Statement of Lieutenant General Kenneth Minihan, United States Air Force and Director of the National Security Agency, to the Senate Governmental Affairs Committee hearing on Vulnerabilities of the national Information Infrastructure, June 24, 1998.

What America must do is find a way to distinguish the difference between structured and unstructured attacks against the national information infrastructure (both the civilian and military portions of it). Our society must establish what the normal "*noise*" level is for it. (13) The Cyber-Posture of the National Information Infrastructure by Willis H. Ware, March 9, 1997, RAND Corporation (MR-976-OSTP).

What parts of the national information infrastructure is vulnerable to attack? Another statement from General Minihan of the NSA gives a brief overview,

"*The resources at risk include not only information stored in or traversing cyberspace, but all of the components of our national infrastructure that depend on information technology .... these include the telecommunications infrastructure itself; our banking and financial systems; the North American power grid; other energy systems, such as oil and gas pipelines; our transportation networks; water distribution systems; medical and health care systems; emergency services, such as police, fire, and rescue; government operations, and military operations.*" (14) Statement of Lieutenant General Kenneth Minihan, United States Air Force and Director of the National Security Agency, to the Senate Governmental Affairs Committee hearing on Vulnerabilities of the national Information Infrastructure, June 24, 1998.

Let us look at two of the more important components of our national infrastructure - the power grid and communication systems.

The North American power grid, which is made up of the nations of Mexico, Canada, and the United States of America, is a very large and complex system. All of its administrative functions are handled via a vast computer network. What happens if an adversary, with the proper personnel, tools, and know-how, attacks the power grid network and shuts it down? Literally millions of people will be left without something that most of us take for granted - electricity!

The telecommunications infrastructure is the other component. The public switched network (i.e., the national telephone system) is a singular point of concern because it provides the bulk of connectivity among computer systems, people, organizations, and functional entities. It is the backbone of interpersonal and organization behavior. (15) The Cyber-Posture of the National Information Infrastructure by Willis H. Ware, March 9, 1997, RAND Corporation (MR-976-OSTP).

The communications infrastructure is particularly vulnerable because it is used for both military and civilian voice, video, and data communications. These systems are controlled by the companies (such as AT&T, MCIWorldCom, Sprint) who own the fiber optics and trunk cable systems that transmit the information. Potential adversaries could hack their way into the AT&T mainframes and gain control of its systems. Once in control, these adversaries could redirect, stop, or disable the systems from operating effectively. This would cause a great strain on American society. Imagine not being able to call you family in another state. Or how about not being able to withdraw money from an ATM because its communication lines with your bank have been disrupted. Or what about communication satellites that are directed to stop transmitting signals. How are military leaders in the field supposed to communicate with their headquarters without secure satellite communications?

"*The Defense Information Infrastructure consists of communications networks, computers, software, databases, applications, and other capabilities that meet the information processing, storage, and communications needs of Defense users in peace and wartime.*" (16) Report to Congressional Requesters, May 1996, Information Security - Computer Attacks At Department Of Defense Pose Increasing Risks, Government Accounting Office / AIMD-96-84, Defense Information Security (511336).

DEFENSIVE STRATEGIES FOR INFORMATION WAREFARE

There are effective ways that America can protect its national information infrastructure. Some of these measures include --

- All components of the Defense Department's infrastructure must be brought up to the same level. This means hardware, software, and personnel. In-fighting between the different service branches needs to give way to co-operation and resource sharing;
- Policies need to be established setting minimum standards and requirements for key security activities; and
- There must also be clearly assigned responsibility and accountability for ensuring that these minimum standards are achieved.

Some of the tools that can be used to safeguard the national information infrastructure include –

- Firewalls are hardware equipment and software applications that protect system resources from hackers. A firewall monitors all incoming traffic and attempts to block all unauthorized intrusions;
- Encryption is the transformation of original data into ciphered (altered) data. Only those who have a key to the encryption program can un-encrypt the data; and
- Authentication can be used for network security to prove that a system user is who he/she is supposed to be and that he/she has a right to use the system. Some examples could be for each system user to identify himself/herself with a finger print or retinal scan identification.

There are several civilian agencies and military commands that are responsible for protecting the national information infrastructure.

The following are some of known agencies –

- In 1988, the Department of Defense established the Computer Emergency Response Team (C.E.R.T.). It is based at Carnegie-Mellon University.
- In December 1992, the United States military initiated its formal Defensive Information Warfare program. Specifics for the program are as yet, available.
- In its December 1995 Defensive Information Warfare Management Plan, the Pentagon defined a three-pronged approach to protect against, detect, and react to threats to the Defense Information Infrastructure. Again, specifics are unavailable.
- In 1996, the Air Force established the Air Force Information Warfare Center (I.W.C.). That same year, the Navy established it's Fleet Information Warfare Center (F.I.W.C.) and the Army established it's Land Information Warfare Activity (L.I.W.A.). The main focus of each of these Commands is to conduct Offensive Information Warfare and to protect the Defense Information Infrastructure against attacks.
- In December 1998, the Pentagon establishes the Joint Task Force for Computer Network Defense. This task force is supposed to be an effort between all of the different service branches to share resources.
- The Defense Information Security Agency (allegedly chartered in the mid-90's) has established a Global Control Center. The Center is staffed by the Automated Systems Security Incident Support Team (A.S.S.I.S.T.) to provide a centrally coordinated around-the-clock Department of Defense emergency response team to attacks on United States military computer systems. Because of the nature of the global information network, A.S.S.I.S.T. can support United States military installations located around the world.
- The National Security Agency is a government agency which is heavily involved in all aspects of Information Warfare. They employ lots of "*code-breakers*" and have their own stable of hackers.

AMERICA'S OFFENSIVE INFORMATION WARFARE CAPABILITIES

Offensive Information Warfare is now being integrated into battle plans along with conventional strategies such as bombing an adversary. The Air Forces' I.W.C., the Navy's F.I.W.C., and the Army's L.I.W.C. are all alleged to be the military commands that will be conducting the Offensive Information Warfare campaigns of the future. The following statement from United States Senator John Glenn sheds some light on America's Offensive Information Warfare capabilities -

"*We are rapidly getting to the point where we could conduct warfare by dumping the economic affairs of a nation via computer networks*." (17) Cyberspace soldiers have a finder on the mouse, Business Times, Technology Section November 2, 1997.

Again, please remember that much of U.S. military's capabilities are unknown to the general public, so I can only outline, in general terms, what they do.

FUTURE TRENDS IN INFORMATION WARFARE

American society is moving more towards full integration of the national information infrastructure. You will pay your bills, perform bank transfers, and make dinner, hotel, or airline reservations from your home PC or a public information terminal. America's national information infrastructure will become a major component of the larger global information network. This System will become more open as more and more people conduct their affairs on-line. But also measures will be taken for system users to identify themselves (retinal scan or fingerprint, if not a DNA sample). Hackers, as always, will find simple and effective ways around these enhanced security measures. They might do things like piggy-back their own programs on the connections that legitimate system users are generating. Another important aspect of the future of cyber space will be the evolution of the hackers. They will evolve into cyber mercenaries. They will advertise their services on the global information network. These hackers will be hired by governments, organizations, and individuals. As for future warfare, instead of threatening another nation-state with nuclear war (physical destruction) governments will threaten to destroy the national information infrastructure of a potential adversary (of course this won't work on organizations or individuals). However, this will be a double-edged sword because as the global information network becomes truly global, a disruption in one node of the System could have unknown consequences throughout the rest of the Network. The is would called, "*cyber collateral damage*." There will be a "*digital*" Pearl Harbor. And there are multiple countries, organizations, and individuals that have the technical know how to devise and conduct such an attack. The United States Department of Defense will continue to develop its own Defense Information Infrastructure. This will be made as secure as possible as the military become more and more dependant on the free (and secure) flow of data to enable it to meet its commitments around the world.

Rob Hiltbrand
rkhbrand@hotmail.com