Global Information Assurance Certification Paper

INFORMATION WARFARE:
A STUDY ON PROTECTING KEY INFRASTRUCTURES TO AVOID DIGITAL DISASTER

By

Andrea Price-Lace
Version 1.4b
GSEC Practical Assignment
Option 1

ABSTRACT:

One need only pick up a newspaper and read the headlines to see the far-reaching effects of attacks launched across the Internet on today's society – the Blaster worm infects one half million machines worldwide, taking out Air Canada and parts of the Mid-Atlantic Railway System, as well as shutting down the Department of Motor Vehicles in the State of Maryland. The Blackout of 2003 illustrates just how vulnerable the aging Northeast Power Grid is and the widespread damage that can be inflicted with its failure. Information Warfare and attacks on America's Key Infrastructures has the potential to affect all aspects of every day life. This paper examines the weapons of Information Warfare, as well as defensive measures that can be implemented as part of a multi-faceted strategy to defend against cyber attacks before a true digital disaster occurs.

INTRODUCTION:

The goal of Information Warfare can be summarized in a passage from Sun Tzu's The Art of War - "To win a hundred victories in a hundred battlefields is not the acme of skill, but to subdue the enemy without fighting is the acme of skill" (1). The technological explosion that has taken place over the past 30 years has led to the Internet becoming the foundation of our information infrastructure. How to balance the ever-increasing need to simplify and accelerate access to information while maintaining a high level of security for critical data has become a major technological challenge.

What is Information Warfare?

According to Dr. Ivan Goldberg, there are two components to Information Warfare - offensive and defensive (2):

> *Information Warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries*

The relative ease with which Information Warfare can be executed is frightening. On a basic level, offensive Information Warfare is a computer intrusion. The technology used to engage in Information Warfare is ubiquitous and attacks may be carried out by anyone with a little knowledge from anywhere on the planet. On a more complex level, attacks may be carried out against key targets critical to our national security in the four main infrastructures – namely the power grid, communications, finance, and transportation (3).

Perception management, malicious code, and predictable responses to attacks are weapons of today's cyber arsenal. The spectrum ranges from false information campaigns to malicious network attacks with trojans, viruses, worms, and denial of service attacks (4).

In 1995, the Security Policy Board issued a report, listing at least 30 countries actively pursuing Information Warfare programs, including: China, Cuba, Egypt, India, Iran, Iraq, Libya, North Korea, Russia, and Syria (5, 6). President George W. Bush, in a Directive signed in July of last year (2002), instructed the United States military to actively pursue a cyber arsenal capable of disrupting foreign computer systems (7). The previously secret directive plans for cyber warfare to follow the current rules of engagement set forth for nuclear warfare, namely the principles of proportionality (whether a given level of force is appropriate in response to a particular grievance and if the action is appropriate in light of its objectives and resulting casualties) and discrimination (targets are acceptable military targets vs. unacceptable civilian targets) (8). In light of the new landscape, battles will no longer be fought only on the traditional battlefield of physical terrain, but in a cyber world with no physical boundaries, where the targets are no longer clearly defined as traditional military targets.

In the changing landscape, business and private industry become fair game with the provision of key infrastructures by the commercial sector, and regulation by the government sector. This creates interdependence between the public and private sectors. With the exploding growth of the Internet, globalization of businesses adds to this interdependence, enabling the problem of Information Warfare to permeate all facets of society.

> *Commercial services from the national information infrastructure provide the vast majority of the telecommunications portion of the Defense Information Infrastructure (DII). These services are regulated by Federal and State Agencies. Local government agencies regulate the cable television portion of the information infrastructure. Power generation and distribution are provided by very diverse activities – the Federal government, public utilities, cooperatives, and private companies. Interstate telecommunications are regulated by the Federal Communication Commission, intrastate telecommunications by the State public utilities commissions (4).*

With deregulation, the private companies competing to maintain the infrastructures rely more on IT to centralize information systems. Reliance on IT dramatically increases a system's vulnerability to attacks, especially denial of service attacks (9). American business practices have led to an increased dependence on Internet-based communications networks, allowing access to the outside world, shifting away from a closed network previously maintained in-house. "This type of system, based on a rather insecure protocol, TCP/IP, has

opened up a whole range of vulnerabilities for hackers and information warriors to target" (10).

Technology has also outpaced the willingness of American business to invest in IT security measures. Common practice is to spend money on emerging technology to increase a company's ability to complete tasks more efficiently, with a blind eye turned toward security. This practice is acceptable until neglecting improvements results in more costly clean-up actions. This can clearly be seen in the dramatically different effects of power outages that hit the power grid of the Northeastern United States, and the power grid in London this summer.

With the infamous Blackout of 2003, millions of people up and down the East Coast from Canada to New York City and inland to Ohio were affected by a breakdown in the electrical power grid, resulting in an estimated $100 billion in damage. Upon further examination, investigators fault aging equipment used to supply electricity and the lack of an updated central power control system. By contrast, National Grid Tranco (NGT), Britain's electricity supplier, was able to minimize the effects of a power outage in London this August. The damage was controlled and power restored within 30 minutes due to IT upgrades made by NGT to the power monitoring and control systems in the early 1990's (11).

Internet Vulnerabilities - The Way to Wage Information Warfare

"The core of our information infrastructure is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network" (12). The tools used for an Information Warfare attack are readily available, with root kits posted on websites for any novice hacker to download and employ from their personal computer for nefarious reasons. This characteristic of Information Warfare is known as Asymmetric Warfare, where a relatively minor investment, i.e. the cost of a PC, can yield exponential results. Asymmetric warfare is exemplified through the success of the Melissa virus. Factor in the cost of an average personal computer and the time taken to write the virus program, someone was able to inflict approximately two billion dollars worth of damage worldwide with minimal investment. In light of this characteristic, it's no wonder the number of identified computer security vulnerabilities, defined as "Faults in software and hardware that could permit unauthorized network access or allow an attacker to cause network damage, "soared over a two year period (2000-2002), with the number of vulnerabilities going from 1040 to 4129" (9).

The multitude of vulnerabilities introduced into previously closed networks with the increased information interdependence and usage of the Internet and TCP/IP Protocol are listed below:

Human Factors
-Information Freely Available
-Poor Password Choices
-Poor Network Configuration
-Disgruntled Employee

Authentication Based
-Password sniffing/cracking
-Social Engineering
-Corrupted/Trusted System

Data Driven
-Email Programs
-Embedded Program Languages
-Remotely Accessed Software (Java, ActiveX)

Software Based
-Viruses
-Program Flaws
-Excess Privileges
-Unused Security Features
-Trap Doors
-Poor System Configuration

Protocol-Based
-Weak Authentication
-Easily Guessed Sequence #s
-Source Routing of Packets
-Unused Header Fields

Cryptography Based
-Inadequate Key Size
-Algorithm Flaws
-Key Management
-Data Capture Before Encryption
-Encryption Turned Off

Denials of Service
-Network Flooding
-Spamming
-Worms

Defense Against Information Warfare – Historical Trends

How does a country like the United States, protect and harden itself against such vulnerabilities? Before cyber security was a catch phrase within the government, the Rand Corporation, a non-profit Think Tank, issued a report in the Mid-1990's suggesting a three-pronged approach to combat Information Warfare. The first step would be to create a national clearinghouse to collect and assess data from cyber incidents. In addition, there should be an institute for testing and evaluating the security features in software programs and computer systems utilized by key infrastructures. The final pillar would be the sterilization of data passing through the infrastructures so that agencies such as the National Security Agency (NSA) could monitor the traffic without collecting data on U.S. Citizens (3).

In light of these recommendations, the evolution of preventive defensive measures enacted by this country against Information Warfare can be traced along a brief timeline, starting in earnest in 1993. The White House began to take notice of cyber threats to the Nation's Infrastructure with the Clinton Administration, and has continued through the current Bush Administration. Some legislative highlights along this continuum include (5,6):

1993 - President Clinton issues Executive Order #12864, establishing the Information Infrastructure Task Force (ITTF) to address "National security, emergency preparedness, system security, and network protection implications" (7)

1995 - Report drafted by the Security Policy Board finds at least 30 countries actively pursuing Information Warfare programs

1996 - NSA forms Information Warfare Technology Center for domestic and military security
- President Clinton issues Executive Order # 13010, establishing a commission to conduct risk assessment to eight critical infrastructure elements. The Federal Bureau of Investigation (FBI) is tasked with leading Interagency response to cyber incidents
-Congress passes National Information Infrastructure Protection Act of 1996, revising the Federal Criminal Code relating to fraud carried out with computers

1999- Establishment of the FBI's National Infrastructure Protection Center (NIPC) to enhance computer security in the public and private sectors (8)
- Cyberspace Electronic Security Act (CESA) establishes new encryption policy with lessened export controls, an emphasis on critical infrastructure protection, and government access to plain text of encrypted communications and stored data (13)

2000- Filipino Computer Science student, author of the "I Love You" virus, escapes prosecution due to the absence of computer crime laws in the Philippines. Prompts U.S. to push and sign the Council of Europe Cyber Crimes Treaty

2001- President George W. Bush establishes President's Critical Infrastructure Protection Board to develop a national cybersecurity strategy with input from the private sector

2002- President Bush signs legislation creating the Department of Homeland Security (DHS)

2003- President Bush signs the National Cybersecurity Strategy

Upon closer examination of the evolution of national defensive measures to counter Information Warfare, there has been a consistent desire by policymakers to heed one of the recommendations made by the Rand Corporation - to have a centralized, national center for the collection and analysis of information relating to cyber security incidents involving critical infrastructure targets. The clearinghouses proposed and/or put into place have been NIPC and

the proposed Federal Intrusion Detection Network (FIDNet)(14). A concerted effort has been made recently to enlist the private sector in a partnership to increase cyber security and provide channels for the sharing and dissemination of knowledge in order to deter future attacks. This trend is clearly defined in President Bush's Cyber Strategy.

The National Strategy to Secure Cyberspace

The goals of Bush's 2003 Cyber Strategy are to:

- Prevent cyber attacks against America's critical infrastructure
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur (9,13,14)

These goals expand upon the aforementioned recommendations made by the Rand Corporation, by setting five priorities: 1) Establish a National Cyberspace Security Response System; 2) Develop a National Cyberspace Security Threat and Vulnerability Reduction Program; 3) Develop a National Cyberspace Security Awareness and Training Program; 4) Secure the Government's Cyberspace; and 5) Develop National Security and International Cyberspace Security Cooperation (9).

The establishment of a National Cyberspace Security Response System cannot be done by the government alone. When an attack occurs, reparations must be made quickly and efficiently. Partnerships with the corporate world and universities must be forged to conduct research and analyze the fingerprints of past and future attacks. With a shared information base, a warning system can be established to minimize damage and enhance recovery during and after an attack. An example of successful partnerships in action was the minimizations of the effects of the Code Red worm in 2001.

The goal of the Code Red Worm was to launch the largest attack in Internet history by targeting an IP address, and redirecting any traffic from users attempting to log onto that IP address to the attacker's site in order to use the unsuspecting machine as part of the attack. Fortunately the plan was foiled as the victim website was able to ask backbone providers to re-route packets to the address to non-existent addresses.

A National Cyberspace Security Threat and Vulnerability Reduction Program would also benefit the public and private sectors by identifying the most prominent vulnerabilities in the networks utilized by all users – from the home user to those responsible for the critical infrastructures. This, coupled with the National Cyberspace Security Awareness and Training Program, would raise the overall awareness level of users in the government, industry, and education institutions as to the vulnerabilities of information systems at all levels. Increased

awareness of such problems will subsequently lead to the training of more security personnel and system administrators, who in turn will make more informed decisions about the proper implementation of security measures to decrease attack routes.

The final priority, National Security and International Cyberspace Security Cooperation, illustrates the acknowledgement that the networks of the world are interconnected. This connectivity allows malicious activity to be launched from any corner of the globe against any target, big or small. Determining where the attack comes from, as well as the ability to punish the attacker(s) have been major stumbling blocks in the international community up to this point. In order to strengthen the United States defense against Information Warfare, we are at the mercy of the cooperation (or lack thereof) from other countries to forge an imposing deterrence to malicious attacks.

Legal Issues to Securing Cyberspace

The benefits of attaining the goals set forth in Bush's Strategy are innumerable. However, the legal aspects of employing a defense to Information Warfare have to be considered. Physical boundaries no longer dissuade attacks, and traditional international and domestic laws do not necessarily apply any longer. Once again, "One of the persistent trends in the related histories of the law and warfare is that whenever war, or civil society in general, has extended into a new environment, such as underwater or aerospace, the law has had to 'play catch-up' to the technology" (13).

International law comes in the form of treaties (Conventional Law) or generally recognized agreements (Customary Law) and is challenged by Information Warfare in four ways:

1) The sort of intangible damage that such attacks may cause may be analytically different from the physical damage inflicted by traditional warfare
2) The ability of signals to travel along international networks or through the atmosphere as radio waves supercedes the concept of national or territorial sovereignty. The ability of law enforcement to trace an attacker across international boundaries is hindered by these same laws of sovereignty, as the investigator is limited to international agreements or to domestic law, if done covertly
3) Information Warfare attacks may be difficult to define as aggressive acts of war, just as it may be hard to define the targets as strictly military vs. civilian (14)

Domestic law implications focus on monitoring activity of certain networks associated with the Nation's Infrastructure, raising several legal issues regarding personal information of American citizens. For instance, the average taxpayer

logging onto http://www.irs.gov to check the status of a refund could be flagged, as the activity would establish a connection to a network within the critical financial infrastructure (15).

Additional privacy and civil liberties issues that arise with monitoring activity include interference with an individual's anonymous actions on the Internet, and the keeping of encryption keys by third parties to allow the government easier access to encrypted material (13). Encryption software currently requires the sender and receiver of encrypted data to have an encryption key. Proposed legislation would require the software manufacturers to provide a key to law enforcement if data believed to be associated with a crime such as a terrorist act was encrypted.

Conclusion:

Taking all of the factors surrounding Information Warfare into account – what it is, how it is carried out, preventive measures to eliminate vulnerabilities, and the legal ramifications of such actions – a broad defense in depth becomes the most plausible solution.

First and foremost, there needs to be a public-private cooperation and coordination to enhance information exchange, awareness training, improved response to incidents, and recovery efforts (9). In addition, international cooperation and coordination, especially between law enforcement entities, should be strengthened and new laws and treaties enacted to develop a strong judicial front against hackers and information warriors to discourage damaging attacks.

Strong security measures on private and public networks should be implemented, such as the installation of firewalls and anti-virus software. Access to critical infrastructure networks should be limited and compartmentalized, with fault tolerance and disaster recovery plans put into place, thus limiting the potential damage to the entire nation should a successful attack be launched. In addition, the new version of the Internet Protocol should continue to build upon the incorporation of encryption and better authentication techniques, such as the use of digital signatures instead of passwords to avoid insider corruption (12). The use of better encryption alone would alleviate some of the legal issues introduced with monitoring activities.

The major limitation to any defensive strategy against Information Warfare will be the ability to respond to threats unknown and unanticipated. By realizing the need for proper training and information sharing, awareness will grow, creating an environment conducive to developing comprehensive security policies that are constantly evolving and adapting to each emerging cyber threat. Only through this type of defense in depth can American businesses and government agencies protect the nation's critical infrastructure data to avert a

national security disaster capable of inflicting damage equivalent to what former White House Cyber Security Czar Richard Clarke referred to as a “Digital Pearl Harbor” (9).

References

1. Tzu, Sun. "The Art of War." New York: Oxford University Press, 1971.

2. Goldberg, Dr. Ivan. Institute for the Advanced Study of Information Warfare Home Page. URL: http://www.psycom.net/iwar.1

3. Lewis, Brian. "Information Warfare." URL: http://www.fas.org/irp/eprint/snyder/infowarfare.htm

4. Defense Science Board. "Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)." November 1996. URL: http://www.cryptome.org/iwd.htm

5. Browning, Graeme. "Infowar." April 22, 1997. URL: http://www.govexec.com/dailyfed/0497/042297b1.htm

6. Washington Post Compilation. " Timeline: The U.S. Government and Cybersecurity." May 16, 2003. URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true

7. Graham, Bradley. "Bush Orders Guidelines for Cyber-Warfare." The Washington Post. February 7, 2003. URL: http://www.washingtonpost.com/ac2/wp-dyn/A38110-2003Feb6

8. Peters, Katherine McIntire. " Information Insecurity." Government Executive. Washington: April 1999, Vol 31, Iss 4; pg 18. URL: http://www.govexec.com/features/0499/0499s1.htm

9. President's Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace. February 2003.

9. Carver, Major Curtis A Jr., "Information Warfare: Task Force XXI or Task Force Smith?" URL: http://www-cgsc.army.mil/milrev/English/SepNov98/carver.htm

11. Morgan, Gareth. " IT Systems Prevented Worse Blackout Misery." August 29, 2003. URL: http://www.vnunet.com/News/1143280

12. Libicki, Martin. "The Future of Information Security." Institute for National Studies. URL: http://www.fas.org/irp/threat/cyber/docs/infosec.htm

13. Dempsey, James, Michael J. O'Neil. "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry." DePaul Business Journal. Vol. 12 (1999/2000). URL: http://www.cdt.org/publications/lawreview/2000depaul.shtml

14. Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. "Information Warfare and International Law. Defense University Press. April 1998. URL: http://www.dodccrp.org/iwilindex.htm

15. Cilluffo, Frank J. "Cyber Attack: The National Protection Plan and its Privacy Implications." Statement to the U.S. Senate Subcommittee on Technology, Terrorism, and Government Information, Committee on Judiciary. February 1, 2000. URL: http://www.csis.org/tnt/test02012000.htm