GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

INFORMATION WARFARE

By Ramlee Sulaiman

(As required for GSEC Examination)

1.0 Summary

This paper will first look at several definitions of Information Warfare before describing the various forms of Information Warfare such as Command and Control, Intelligent-based, Psychological, Economic Information, Electronic, Hackers and Cyber Warfare. This paper will also cover the four principles of Information Warfare and then identify who are the possible users of Information Warfare and the weapons they could possibly used to achieve their objectives. This paper will then look at how the weapons could be used to achieve desired objectives by using the four basic strategies in Information Warfare such as Denial of Information, Deception and Mimicry, Disruption and Destruction, and Subversion. From the basic strategies, I will then define the two types of Information Warfare and then look at the challenges in defending against information warfare attacks.

This paper concludes that Information Warfare is real and defending against the attacks in its many forms involves many parties. The failure of one may have a domino affects onto others.

2.0 Definitions

What is Information Warfare? There will be no one correct answer to this question. Persons with different background will give different answers; probably trying to relate to what business they are in. Those in corporate world might consider Information Warfare as attempts to block critical information from reaching their competitors. Doing so would then slow down the capability, if not jeopardizing, the business of their adversaries. The general public might see it as a "war" on the Internet but in the military perspective it could mean different thing.

The DoD of United States [1] defines Information Warfare as follow:

> "A*ctions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks."*

© SANS Institute 2000 - 2005 Author retains full rights.

The DoD [2] further defines the information superiority as

> *"the capability to collect, process, disseminate an uninterrupted flow of information to achieve or promote specific objectives over a specific enemy while exploiting or denying that ability to the enemy*."

Winn Schwartau [3] in his book *Information Warfare*, however, describes Information Warfare in different way. He splits the definition of information warfare into three classes, Personal, Corporate and Global.

He describes the first class as attacks against an individual's electronic privacy. This includes the disclosure of digital records and database entries wherever information is stored. The information obtained could be used for the purpose of blackmailing or to destroy the integrity of a person.

The second class was described as competition between corporations around the world. It is done at bigger scale then the first class and with wider objectives. One mobile telecommunication company would try to interfere with the transmission coverage of another company to create dissatisfaction among the subscribers with the hope to lure them to switch to the former network. Shutting down a computer network of a competitor would bring down their business too. The extent of damage possible, however, depends on how critical is the computer network to the affected corporation.

Global, the last class of Information Warfare as defined by Winn Schwartau, involves works against industries, global economic forces or against entire countries or states. For example, the economic embargo against Iraq after the Gulf War brings down the economic and industries of Iraq, putting his population in severe sufferings. The WTC attack on September 11 did not only attack the economy of United States but brings down along with it, insurance companies through out the world.

Reto E. Haeni [5] however looks at Information Warfare in different perspective. He started his argument with the three waves of warfare, agrarian, industrial and information waves. The agrarian wave is when war is fought by part time warriors for their landlord during certain period of the year for more piece of land or food. They use home-made weapons as such the damage done is not devastating.

The industrial wave comes along with the industrial revolution where new weapons are developed to create more damage to the opposing forces. The war is more organized where soldiers are properly trained and earn a fixed salary. The war in this wave creates more devastating or catastrophic damage as we see in the World War 2 when atomic bombs exploded in Hiroshima and

© SANS Institute 2000 - 2005 Author retains full rights.

Nagasaki.

Reto E. Haeni sees the war in information wave will no longer produce a mass destruction but the deletion of critical data.

So, what is Information Warfare? I believe Information Warfare is all about deception against the enemy. It involves the information itself, the information processes, the information infrastructure, the people and leaders. On the other hand, Information Warfare is also about providing accurate and timely information to our leaders to assist them in the decision making processes and thereafter, should be able to pass down that decision for execution by the people.

3.0 The Many Forms of Information Warfare

Information Warfare is not a separate technique of waging war, neither in the military perspective nor the general public. It consists of various forms, which combine together to make up a larger concept. Martin Libicki [4] has identified seven forms of Information Warfare as follow:

- Command and Control Warfare (C2W),
- Intelligent-Based Warfare (IBW),
- Electronic Warfare (EW),
- Psychological Warfare (PW),
- Economic Information Warfare (EIW),
- Hackers Warfare (HW) and
- Cyber Warfare (CW)

Command and control is a very important aspect especially in the military organizations. Situational awareness is vital for the commanders in order to make a correct decision in critical situations. Failure to obtain precise and timely information from the ground would hamper the decision making processes of the commanders. So, the commanders and communication link are the issue here. Both need to exist for the troops to function effectively. It is obvious here that in order to achieve an objective of a military operation, the enemy leader needs to be fed with corrupted information, if not killed, or the communication lines need to be compromised or destroyed. At the same time, we need to protect our own.

IBW is not about intelligent gatherings but about intelligent information derived from devices or sensors that are fed directly into an operation. Satellite images that display the movement of opposing troops would determine the course of actions that need to be taken by other party. Intelligent weaponry system would reduce the workload of battling troops. They just “fire and forget” and sensors installed in the weapon system would lead the way to the predetermined targets. If the sensors could be compromised, it could just turn its way back on

© SANS Institute 2000 - 2005 Author retains full rights.

us!

EW has been long in the history of warfare. It deals with electromagnetic radiation with the main objective is to degrade the physical basis for transferring information. EW is used to search for identity and locate sources of radiated electromagnetic energy, to attack on personnel, facilities or equipments and to protect own personnel, facilities and equipment from any effects of EW employment.

Psychological Warfare involves the use of information against the human mind. Television, radio and internet play very important role in psychological warfare. The general population of the United States might not support the attacks on Iraq and Afghanistan if not because of the continuous portrayal of how bad those leaders are. Seen is believing and that's what the United States, through CNN for example, is doing. The reformation movement in one of South East Asia nations is an example of psychological warfare against the opposing commanders or leaders. The leaders of the ruling parties are painted with all sorts of corruptions, power abuses, cronyism practices etc. The ruling parties, on the hand, use television, newspapers and radio to counter the attack by the oppositions and at the same creating fear to the general public should the nation comes under the control of the opposition. In psychological warfare, the truth is not important as long the objective or desire of the leaders is achieved. What is "white" today could be considered "black" tomorrow!

Economic Information Warfare consists of information blockade and information imperialism. An information blockade works by forcing the target country to work in the dark and in the long run, removing the benefit of information exchange. The impact could be disastrous to nations that depend so much in information technology. Cutting down their communication lines would bring down their business to a halt. Believing in information imperialism means believing that trade is war. Nations struggle with one another to dominate strategic economic industries. Some industries are better than others. The quest for control of oil in the Middle-East could be one the reasons of the region instability for such a long time. A more powerful nation would try to dominate the oil producing nations for their own interest through "velvet glove" or "iron fist".

Hacker warfare varies considerably. It could be done by an individual or group of individuals with a common objective. It is not news anymore to hear about a web site being defaced, credit card information being stolen through the internet. It happens during the Gulf War where military sites of United States being hacked and information stolen and in fact offered to Saddam Hussein [10]. In the Hackers Warfare, the attackers can be on site or anywhere that we could imagine and he could be our neighbor who lives just next door. It just a matter of getting the right tools and nobody is safe as long as you are connected to the internet.

© SANS Institute 2000 - 2005 Author retains full rights.

CW is new and it comes along the rapid proliferation in information technology. The soldiers may not have to carry heavy weapons anymore but light digital equipments that could assist them in achieving their mission. With the advanced technology in computer simulation, a war could be rehearsed to get the best strategy to win the war. The pilots, for example, could just "fly" their aircrafts in the simulator to get familiarize with their operation areas before they actually do it in the real world.

4.0 The Principles of Information Warfare

Daniel E Magsig [8] has listed the principles of Information Warfare as follow:

- Denial,
- Force Enhancement,
- Survival Situational Awareness and Command, Control and Communications and
- Level.

Information about the strength and weakness of the enemy, own and friendly forces is important in order to win a war. Denial of that information to the opposing commanders would put them in the dark. Therefore, the command and control centers, decision support and communications systems should be the primary targets and all hostile sensors should be suppressed or destroyed before engaging in combat.

The second principle is Force Enhancement. The troops on the ground need the information as much as their commanders do. The flow of information from top down should be as smooth as possible to reduce or avoid additional risk to the troops.

Decentralization is important to ensure survivability. The policy and strategy should be centralized at the top level but leeway should be given to lower level to plan and execute their missions. Interoperability is another aspect to ensure survivability. All information and communication system should be able talk to each other to allow maximum sharing of information.

The last principle of Information Warfare is Level states that all available technology should be used against enemy forces immaterial of the capability of the enemy. The intensity of information warfare conflicts should be all out efforts. The war has never been and will never be, fair!

5.0 Who Would Use Information Warfare?

So far we have look at various definition of Information Warfare, its many forms and principles. The question now is "who would use the Information Warfare?" The US DoD [4] has categorized the users as follow:

© SANS Institute 2000 - 2005 Author retains full rights.

- Insiders and authorized users;
- Criminals and Organized Crime;
- Foreign Countries;
- Terrorists;
- Industry and Economic Espionage; and
- Hackers.

These six categories of users might not work alone. One category of users might be co-operating with another group(s) of users militarily or technologically at strategic or organizational level. Dr David S Albert [7] describes these interactions among the users in three dimensions as follow:

- Nature of Interaction,
- Arena of Interaction and
- Level of Interaction.

The nature of interaction explains about the possible cooperation among users of different category to achieve their common objectives. They could also compete and may be at war with one another if they could not come to an agreement with one another.

There are many areas where one user could interact with another. Those areas could be in military, political, economic, social, technology and also in ideology or religion. Each area of interactions might have a different objective and impact.

Looking in other perspective, these users could be interacting at public, strategic, operational or tactical levels. They could also interact globally, international, national or organizational level. The September 11 incident could be the result of this interaction. However, with the present technology, one could do it alone.

6.0 The Possible Information Warfare Weapons

Reto E. Haeni [5] has listed down a few examples of the possible weapons that could be used by the military and terrorists as follow:

- Computer Viruses

  "A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces." [6]

- Worms

© SANS Institute 2000 - 2005 Author retains full rights.

"A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs."[6]

- Trojan Horses

  "A Trojan horse is a code fragment that hides inside a program and performs a disguised function. It's a popular mechanism for disguising a virus or a worm"[6]

- Logic Bombs

  "A bomb is a type of Trojan horse, used to release a virus, a worm or some other system attack. It's either an independent program or a piece of code that's been planted by a system developer or programmer."[6]

- Trap Doors

  "A trap door, or a back door, is a mechanism that's built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection."[6]

- Chipping

  The manufacturer can easily configure chips so that they contain some unexpected functions. They could be built so that they fail after a certain time, blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location.

- Nano Machines and Microbes

  Nano machines and Microbes provide the possibility to cause serious harm to a system. They could be used to attack the hardware of a computer system.

- Electronic Jamming

  It is used to block communications channels at the enemy's equipment so that they can't receive any information.

© SANS Institute 2000 - 2005 Author retains full rights.

- HERF Guns - EMP Bombs

  HERF stands for High Energy Radio Frequency. HERF guns are able to shoot a high power radio signal at an electronic target and put it out of function. The damage can be moderate or severe. In essence, HERF guns are nothing but radio transmitters that send a concentrated radio signal to the target.

  EMP stands for electromagnetic pulse. The source can be a nuclear or a non-nuclear detonation. It destroys the electronics of all computer and communication systems in a quite large area. The EMP bomb can be smaller than a HERF gun to cause a similar amount of damage and is typically used to damage not a single target but all equipment near the bomb.

- Van Eck Radiation.

  It is the radiation that all electronic devices emit. Specialized receivers can pick up this radiation and tap a wealth of information. Fortunately, there are various safeguards against this type of attacks.

- Cryptology

  Cryptology is a weapon of information warfare designed to encrypt and crack secure communications respectively. Despite significant advances in cryptography, cryptanalysis will continue to be an important weapon aided by equally significant advances in computing power.

- Video Morphing

  Video morphing is a weapon that could be used in a manner to make an enemy leader appear to say things he or she didn't in fact say with the purpose to undermine credibility.

7.0 The Basic Strategies in Information Warfare

The principles of Information Warfare explain what need to be done to win an information war. The strategies here explain how it is to be done. The four basic strategies [9] are as follow:

- Denial of Information,
- Deception and Mimicry,
- Disruption and Destruction and
- Subversion.

© SANS Institute 2000 - 2005 Author retains full rights.

One user would not want other party to have access to their critical information. The use of Firewall, Intrusion Detection system, Virtual Private Network, encryption and of late, steganography are the manifestation of the effort to deny efforts by the enemy forces to have access to own information.

At the same time, hackers, terrorists and foreign countries are developing new tools everyday to get into the heart of the enemy's information systems with the intention to insert misleading information or program to create dysfunction, alternately the outright destruction. Any denial of service attack, from "ping of death" to an EMP bomb could be implemented to achieve the desired objectives.

Subversion is a strategy where information is inserted into the opponent's system that would trigger a self-destructive process such as logic bomb, virus and other destructive programs that use system resources to damage the system itself.

8.0 Types of Information Warfare

Let's look at the definition by the US DoD again. It has two components; one is to affect the adversary and second is to protect our own. From the definition we can now derived that there are two types of Information Warfare. First is to attack or being offensive and second, is to defend our own or being defensive.

The principles and strategies as discussed above should now be studied in two different perspectives. Defensively, the principle of denial means that we should deny the enemy forces to come close to our command centers and communication lines, either logically or physically. Our sensors should be as stealthy as possible to avoid detection.

Having achieved the first principle, to achieve the second is much easier. When the flow of information from the top to bottom or along the same line is uninterrupted, the force enhancement could be achieved.

Situational awareness and interoperability is another important principle of information warfare. The commanders and troops on ground should be looking at the same picture. With decentralization, one command centers destroyed would not jeopardized the survivability of the required situational awareness. Interoperability however requires proper planning especially in the procurement and implementation processes.

The last principle, level, would ensure that all level of our forces will be equipped with latest technology. It should come together with proper training.

Offensively, all the four principles of information warfare would attempt to create

© SANS Institute 2000 - 2005 Author retains full rights.

confusion to the commanders and the troops on ground by destroying or compromising the communication lines. With the use of all technology available, the war could be ended sooner to reduce the loss of lives and other assets.

As for the strategy, the Denial of Information could mean to deny the enemy of our critical information by securing our system effectively and at the same time, offensively, denying the flow of information between the enemy commanders and their troops.

Defensive is of course more difficult as more tools are developed every day in line with the rapid advances in technology. The offensive is always way ahead in this race as the offensives can choose the time, place, tools and techniques for the attack.

9.0 The Challenges of Information Warfare

As mentioned earlier, defending against Information Warfare is not an easy task due to many reasons. Society and organizations need to really understand the nature and characteristics of the threat. It is difficult to convince the top managements until something happens. On the other hand, system administrators would try to hide any incident for fear of losing their jobs.

To launch information attack does not cost much. Many tools are readily available at the internet for free and it could be done by anybody from anywhere in the world. Various laws and regulations are introduced to deter the attack but to implement or enforce the laws and regulations are easier said than done.

Improving the ability to see an attack coming or providing indications and warning of attacks in a timely fashion is perhaps the most difficult challenge. An intrusion detection system or firewall would helps but without strong policies and stringent monitoring, it won't be effective. To have a 100 percent secured system is impossible.

10.0 Conclusion

The threat of information warfare is real. The low cost of mounting these attacks, especially in computer network environment, has made defense a very difficult challenge. This situation is getting worse with the rapid proliferation of information technology and know-how. As more computers are connected to networks as the need for connectivity increases, vulnerabilities would also increase.

Given this situation, we need to find a way to protect our systems against catastrophic events. The first step that needs to be done is develop better understanding of the nature and characteristics of the threats among the people

© SANS Institute 2000 - 2005 Author retains full rights.

in our organization as the people are always the weakest link.

11.0 References

[1] The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) Number 3210.01, dated 02 January 1996

[2] US DoD, *Joint Pub 3-13 Joint Doctrine for Information Operations*, 9 October 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

[3] Schwartau Winn, *Information Warfare, Chaos on the electronic superhighway*, (Thunder's mounth press 1994) http://www.infowar.com/freednlds/Chaos_IW1.zip

[4] Martin Libicki, *What is Information Warfare*, National Defense University, 1995. http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html

[5] Reto E. Haeni, *Information Warfare – an introduction,* January 1997. http://www.seas.gwu.edu/~reto/infowar/

[6] Russel Deborah and Gangemi G.T., *Computer Security Basic*s, (O'Reilly & Associates, 1994)

[7] Dr. David S. Alberts, *Defensive Information Warfare*, NDU Press Book, 1996. http://www.ndu.edu/ndu/inss/books/diw/index.html

[8] Daniel E Magsig, *Information Warfare In The Information Age*, 1996.

[9] Carlo Kopp, *Information Warfare*, http://www.infowar.com/info_ops/00/info_ops033000b_j.shtml

[10] Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999.

© SANS Institute 2000 - 2005, Author retains full rights

© SANS Institute 2000 - 2005 Author retains full rights.