Global Information Assurance Certification Paper

Tim Kroeger
GSEC version 1.4b

Information Warfare: More than meets the eye

Abstract

This paper will cover an arena of areas dealing with Information Warfare (IW) to include the Department of Defense's position on and use of Information Warfare. A leading subject matter expert on Information Warfare, Martin Libicki, discusses his concept of Information Warfare consisting of the following seven sub-areas; Electronic Warfare (EW), Intelligence Based Warfare (IBW), Hacker Warfare (HW), Command and Control Warfare (C2W), Psychological Warfare, Economic Information Warfare and Cyberwarfare (Libicki).

Introduction

What exactly is Information Warfare (IW)? Is Information Warfare…computer hackers bombarding corporate America? It could be, computer hacking is just one small aspect of Information Warfare. Information Warfare covers a broad subject and usually it only gets one-sided coverage. Too often these days all we hear about is how computer hackers have hacked into a bank or how a new virus has infiltrated our home and business computers. Americans read the paper, listen to the radio and watch the daily news only seeing and hearing what the media's perception of what Information Warfare is. The focus and purpose of this discussion is to introduce you to the remaining areas of Information Warfare.

Operational Security (OPSEC) and Information Security (INFOSEC), also play a key role in Information Warfare. To protect your assets from an attack, you need to have a firm understanding on these topics and implement them in your daily personnel and business routine. By the time you are done reading this paper, your understanding of Information Warfare will help protect you and your company.

Operations Security & Information Security

Before, we start discussing the different areas of Information Warfare, it's important to know and understand what Operations Security (OPSEC) and Information Security (INFOSEC) are. I refer to OPSEC and INFOSEC throughout this discussion as methods to protect you against Information Warfare.

Operations Security (OPSEC)

OPSEC is the process of denying information to adversaries about capabilities or controlling and protecting unclassified evidence of the planning and execution of sensitive activities (ITS). OPSEC focuses on having a good understanding of enemies decision maker's ability to collect reliable, adequate, and timely intelligence and, when integrated with other capabilities, it can shape to our advantage the adversary's knowledge and beliefs about our operations. To implement OPSEC effectively, it's important to have an effective security awareness program. Most people are unaware of what they can and can't say on the phone or in emails. Some key items that should not be discussed in an unsecured manner are:

- Usernames and/or passwords
- Specific network configuration, which could include internal IP addresses and placement of perimeter security devices.
- Specific private information related to key decision makers.
- Any critical information that if, in the wrong hands can, be detrimental to your company. (i.e. roll-out dates for new products or drawbacks due to competitor success)

It is clear from these examples that OPSEC is a critical part of everyone's daily routine and justifies why you need to develop ways to protect critical information that if in the wrong hands can be detrimental to you or your company. OPSEC is an ongoing process that affects our daily routine and needs to be constantly revisited and reviewed to ensure we are protecting the right vital information.

Information Security (INFOSEC)

Information Security merges the technology and techniques of computer security, communications security, emanations security, physical security, and personnel security to protect data, services and other resources. One of the first steps to making INFOSEC work for you is to put together a policy for you and your company. An effective INFOSEC policy should cover some of the following areas:

- Responsibilities; who is responsible for implementing and administering the security policy.
- Anti-Virus policy and update guidelines.
- Specific guidelines for your users to include use of e-mail and the internet.
- Firewall and Intrusion Detection System (IDS) policy
- Define a backup policy

These are just a few examples what should be contained in an effective INFOSEC policy. Like OPSEC, user awareness is critical to making INFOSEC work for you. What good is it to define guidelines for your users if they don't know or understand what the policy is? Understanding INFOSEC is important in

guarding yourself against Hacker Warfare and other attacks against your information systems.

We have discussed the importance of OPSEC and INFOSEC and how it integrates with Information Warfare. It's important to have a understanding of these topics to guard against Information Warfare.

Definition

To properly digest Information Warfare, I need to ensure you thoroughly understand how the Department of Defense defines and uses Information Warfare and how one author, Martin Libicki, expressed his concept throughout key areas.

Department of Defense definition and use of IW

The Department of Defense's definition of Information Warfare was taken from Joint Publication 1-02:

Information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries (JP 1-02).

According to this definition, Information Warfare is nothing more than Information Operations used during times of war to achieve a specific goal. So what exactly is Information Operations? According to Joint Publication 3-13 Information Operations are:

Actions taken to affect adversary information and information systems while defending one's own information and information systems.

To break Information Operations (IO) down even further, Joint Publication 3-13 states that there are two major subdivisions to IO, defensive IO and offensive IO. Offensive IO's main goal is to affect adversary's decision making process while defensive IO's main goal is protect friendly information and information systems. There are a large number of supporting sub-areas to support offensive and defensive IO which are illustrated in Figure 1.

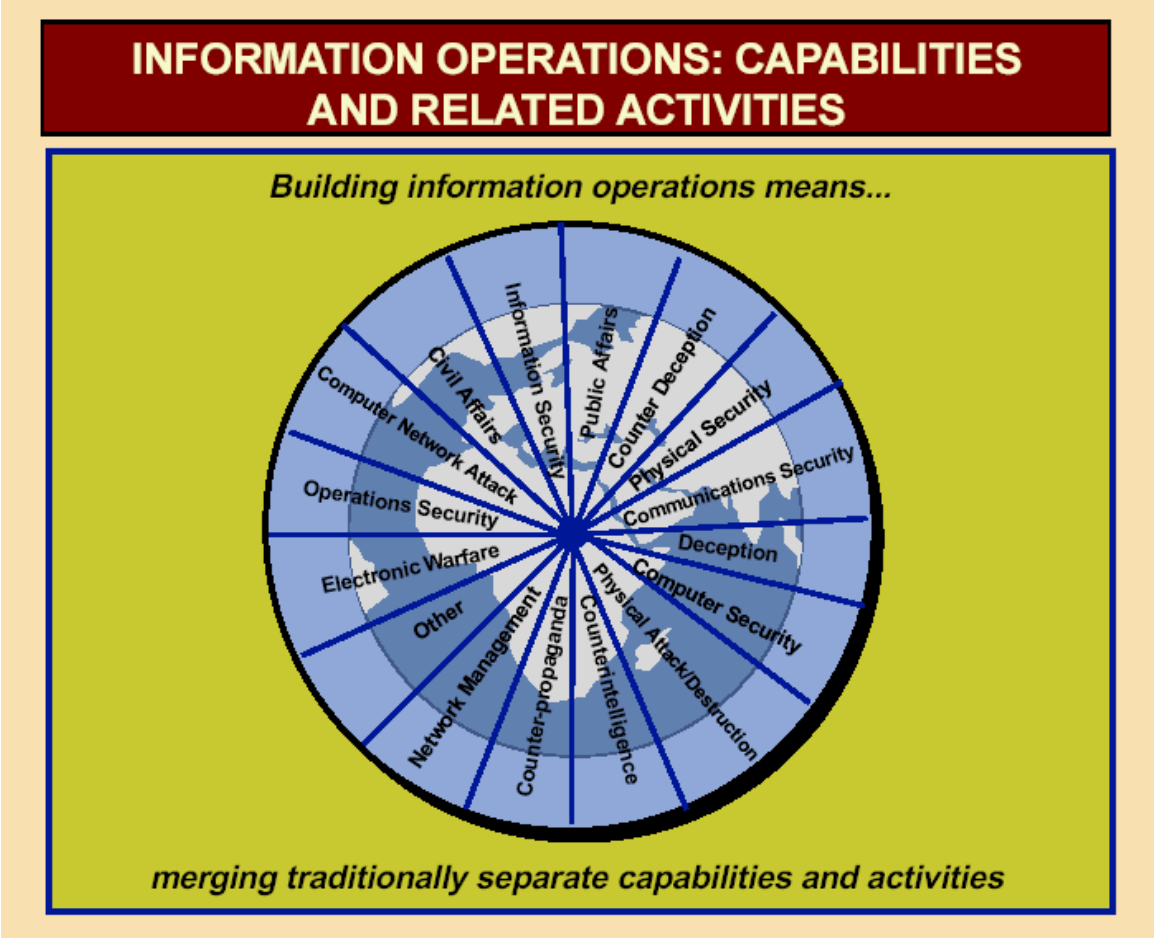

Figure 1

Looking at figure 1, we see Information Warfare or Information Operations covers a vast area of subjects. The key point to figure 1, Information Warfare: Capabilities and Related Activities, is Information Warfare is more than Computer Network Operations i.e. hacking. It's also important to realize Computer Network Operations is a relatively new area of Information Warfare and the Department of Defense is still trying to integrate it into the current IW structure.

Traditional Definition

Now that we looked at how the Department of Defense defines Information Warfare and Information Operations, let's take a look at how Information Warfare is defined by several professionals and experts on the topic. IW can be described as "a struggle over the information and communications process" (Lewis). The best definition of Information Warfare that I have seen to date is by Dr. Ivan K. Goldberg.

> "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" (Goldberg)

In Dr. Goldberg's definition, he states that Information Warfare is waged to achieve advantages in military or business adversaries. Throughout this discussion, you will see areas of Information Warfare that would be easier to use on the military battlefield or in the corporate world. The important point to remember is that Information Warfare can be used on the battlefield or in corporate America at any time. For example, some people who are reading this will have the mindset that "Electronic Warfare can never be used against me or my business; I'm not on the battlefield". That's a bad mentality to get. If your adversary can figure out how to use Electronic Warfare against you to gain an edge over your business, then they probably will.

Electronic Warfare

Electronic Warfare (EW) is any military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum (Lexicon). Electronic Warfare is broken down into three sub-areas. Electronic Attack, Electronic Protect and Electronic Support. Electronic Attack (EA) are actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception. Electronic Protection (EP) are actions we take to counter an enemy's use of EA against us. Electronic Support (ES) provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing.

If you are like me, you are probably saying "How in the world does the electromagnetic spectrum affect me"? Figure 2 is a small portion of the electromagnetic spectrum. The portion I selected contains the frequencies for radios, televisions and cell phones.

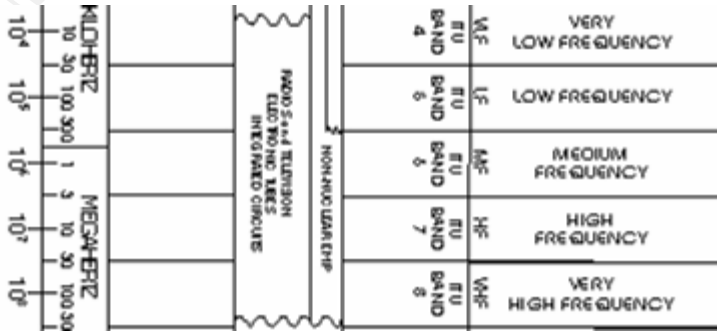

Figure 2

A corporate enemy could either jam these frequencies or listen in to your cell phone conversations to determine how your new product is designed and when it is going to be released. As you can see, Electronic Warfare can be devastating to your business when used against you. One way to protect yourself or your business against Electronic Warfare is to use Operation Security (OPSEC) by avoiding discussions of sensitive information over the phone. Another way to protect yourself or your business is to look into frequency hopping cell phones to counter the threat of being jammed. Electronic Warfare is one of the areas of Information Warfare that you probably will expect little threat from to yourself or your business, but remember that anyone with a scanner and a little patience can be very devastating to you and your company.

Command and Control Warfare (C2W)

C2W is the use of OPSEC, military deception, psychological operations (PSYOP) and electronic warfare (EW) to deny information, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. An easy way to understand C2W is to compare it to the human body. The human body cannot function without the brain. That's what C2W is, an attack against the decision makers of a country or a company. On September 18, 2000 Irwin Jacobs, the Chief Executive of Qualcomm, had his laptop stolen with some sensitive information stored on it (Schiffman). This probably was nothing more than corporate espionage by one of Qualcomm's competitors which would be an example of Command and Control Warfare, an "attack" on a company decision maker. There are no guaranteed defenses against C2W, but a company could guard against this type of warfare by ensuring their decision makers are using encrypted phones or are using some form of encryption on their laptops. Another way to protect you and your business is to make sure the decision makers understand Operational Security and Information Security. History has shown that often the top decision makers are the worst offenders when it comes to Operational Security and Information Security. A strong security awareness program will go far when it comes to defending against C2W.

Psychological Warfare (PSYWAR)

Psychological Warfare are planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of organizations, groups, and individuals (Psywarrior). Psychological Warfare can consist of dropping leaflets on the targeted audience to obtain the desired effect or goals. An example of a leaflet is shown in Figure 3.

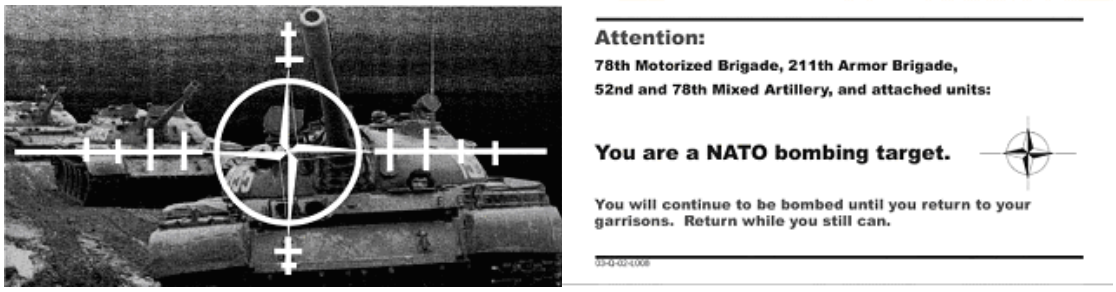

Figure 3

Psychological Warfare can also be waged with loudspeakers on the back of tanks or trucks or from 30,000 ft overhead in a flying television station named Commander Solo. Commander Solo is an EC-130 aircraft flown by the 193rd Special Operations Wing of Harrisonburg, PA which has been flying over Afghanistan recently broadcasting messages like the one quoted below to the Taliban (Psywarrior).

"What are you using, obsolete and ineffective weaponry? Our bombs are so accurate we can drop them right through your windows." (Checkpoint)

Psychological Warfare can be waged in the corporate arena also. An example of corporate Psychological Warfare could be a simple website stating that the date for a new technology has been moved up when it really hasn't or that your competitor is working on breakthrough technology. Both of those examples are meant to provoke some kind of reaction in your thinking and actions meant to provoke or persuade you one way or the other. The best protection against Psychological Warfare is to keep your employees and your customers informed of current company trends and decisions. In Psychological Warfare, the first company that informs the public on key decisions usually builds the confidence and trust of the people.

Hacker Warfare

Hacker Warfare is probably the most familiar portion of Information Warfare for most of us. This type of warfare is also known as Computer Network Operations (CNO) and is often portrayed in movies and headlines. Hacker Warfare is one of the biggest areas of IW where the military and civilian lines get mixed up and you start to see military attacks on civilian companies to gain a desired affect on an enemy. For example, to slow production of tanks for an enemy's army, our military could launch computer network attacks against the company's production line computers. There are two areas of Hacker Warfare, offensive and defensive. Offensive or Computer Network Attack (CNA) is defined as operations to disrupt, deny, degrade, or destroy information in computers and computer networks, or the computers and networks themselves (JP 1-02). Computer Network Attack can originate from an organized hacker group, a nationally supported hacker group or an individual. Nationally supported hacker activity appears to be on the rise. For example, from May 1 to May 8 2001,

China launched a hacker war on the US in retaliation to US hackers attacking Chinese websites after an US EP-3E crash-landed at a Chinese airbase (Heng). Defensive or Computer Network Defense (CND) can be defined as measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction (JP 1-02).

What exactly are you doing to stop the hackers from infiltrating your information systems? Any time you install a firewall or anti-virus software, you are performing Computer Network Defense. You are protecting yourself from Computer Network Attack. Protection against Computer Network Attack can include firewalls, Intrusion Detection System's (IDS), up-to-date anti-virus and an effective computer security policy. All of the above should be included in your company's Information Security (INFOSEC) policy and your personnel information systems. Always remember, there are no boundaries when it comes to Information Warfare.

Economic Intelligence Warfare (EIW)

EIW is one of Libicki's core areas of Information Warfare (Libicki). EIW can be defined as the economic impact of Information Warfare on a country or company. Libicki states that there are two areas of EIW, information blockade and information imperialism. Information blockade is a blockade of information channels similar to an economic blockade. A nation or company would cut-off the targeted countries access to outside information. This blockade would hopefully cripple the economy of the targeted nation.

Information imperialism can be defined as nations holding new technology or information within its borders to offer national companies an advantage over competing companies. Whether information blockade or information imperialism can be called war is a debatable question. At first look, I didn't think that EIW was a core area of Information Warfare, but if you look at the desired result of EIW, it could be used to the adversaries advantage.

Every information warfare campaign has objectives. The objectives could be to cripple a country's air-defense capability or to stop your competitor from releasing a new product on time. To achieve the desired result of Economic Information Warfare, an enemy could use Hacker Warfare or one of the other types of Information Warfare stated already. Defense against Economic Information Warfare would be included in the defenses already listed, again Operations Security and Information Security are crucial in defense of any type of Information Warfare.

Cyberwarfare

Cyberwarfare is an area of Information Warfare that I don't feel rates it own sub-area. Libicki says that cyberwarfare is made up of information terrorism, semantic attacks, stimula-warfare and Gibson-warfare (Libicki).

Information terrorism is when terrorists use your personnel files to blackmail you or to expose you. Semantic attacks are similar to hacker warfare, except in hacker warfare the ultimate goal is to bring down a system and in semantic warfare a system is infiltrated and provides realistic responses, so you don't know it has been attacked. Stimula-warfare is a simulation of an actual war. The simulation would demonstrate who would win a physical war. The last area of cyberwarfare is Gibson-warfare. Gibson-warfare is a virtual battle between two parties. Like in the movie "Tron", the parties would fight in a virtual arena. Libicki also goes on to say that the global infrastructure is still not developed enough for this type of warfare, but says that in the Victorian era they had similar discussions about air warfare.

My personnel feeling is that cyberwarfare is too "movie-like" and we won't see it on any large scale. You might hear about one or two people being blackmailed because of the information that was found on their desktop, but for the most part cyberwarfare is not realistic. That doesn't mean that you shouldn't look at the possibilities of cyberwarfare and start to protect yourself now. You can start to defend yourself by ensuring you have an effective Information Security policy which includes firewalls, encryption of critical information and IDS's to monitor traffic inside and out of your network.

Intelligence Based Warfare (IBW)

Intelligence Based Warfare is a unique concept. When I think of intelligence as it relates to Information Warfare, I think of it in a supporting role. Libicki states that "IBW occurs when intelligence is fed directly into operations (notably targeting and battle damage assessment), rather than used as an input for overall command and control (Libicki)." As far as I'm concerned the only way that intelligence relates to Information Warfare is in a supporting role of all the facets of IW. Take C2W for instance, you wouldn't know what parts of the network to destroy in order to disrupt decision making if you didn't have good intelligence.

In EW, you wouldn't know what parameters to look for on a specific radar if intelligence hadn't supplied you with the information. In figure 4, I've drawn how I think intelligence fits into Information Warfare.

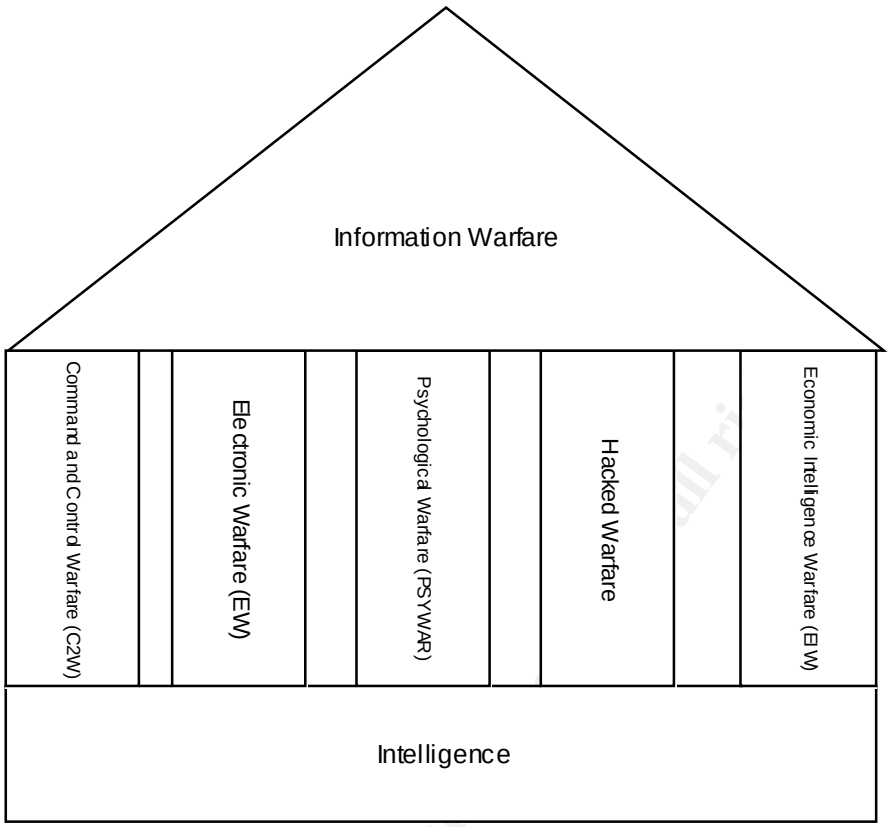

Figure 4

As you can see from figure 4, intelligence supports every area of Information Warfare. Without intelligence, I believe you wouldn't be able to succeed in the five areas of information warfare; C2W, EW, PSYWAR, Hacker Warfare and EIW. To properly defend yourself against intelligence, you have to understand how the intelligence is gathered against you. For the enemy to successfully use intelligence against you or your company, they have to gain specific knowledge related to your company. For example, in Hacker Warfare, we know that port scanning and probing is a way that intelligence is gained against your network defenses. One way to counter scanning and probing is through use of firewalls and/or honeypots.

Social engineering is a technique used to get your workers to divulge critical information related to your company. The key is to know how the enemy will gather intelligence, so you can protect yourself against it. Remember for any of the different Information Warfare sub-areas to be used effectively against you, the enemy has to know what your weaknesses are to exploit them. In order to protect ourselves, you must know your weaknesses and either fix them or accept the risk of not fixing them. It's crucial to periodically assess your total security posture against known and unknown threats. I hope by now you can see how Operations Security and Information Security are critical in protecting yourself against intelligence gathering. One of the biggest protections against intelligence

gathering is awareness. Educate your workers on how information can be gathered and what your enemies are looking for. When properly armed with this information, you and your co-workers can protect yourselves against intelligence gathering methods.

Information Warfare vs. Conventional Warfare

Throughout this paper, I know some of you are probably wondering how Information Warfare compares to Conventional Warfare. First of all, information warfare is not a substitute to conventional warfare; it enhances our war-fighting capability. Information Warfare is designed with a specific goal in mind to aid conventional warfare in a specific area. In the case of C2W, we could knock out the head air defense node, allowing our bombers to go in and bomb key camp areas. Information Warfare and conventional warfare go hand in hand. That is probably the biggest misconception that I've seen in reports and articles on the web. They usually indicate that information warfare is separate from conventional warfare and do not relate. In fact, the opposite is true; Information Warfare can be used to obtain an advantage in an operational, tactical or strategic war.

How Does IW Affect You?

I know some of you are thinking "This paper is very informative, but I'm still only concerned with the hackers trying to get into my networks". Information Warfare affects all of us on a daily basis. Recently terrorists have been waging Information Warfare on America, whether we realized it or not. Look at the shoe-bomber for instance. How many airports checked their passenger's shoes for explosives before he was discovered? Now, after the shoe-bomber how many of us are lucky enough not to get our shoes checked? Why? The shoe-bomber didn't even blow anything up. People are afraid to fly because of the shoe-bomber. This in turn is affecting our air industry, which is affecting airplane makers and all the industries that support both of those markets. This is an example of Psychological Warfare at work. The terrorist didn't actually blow up the airplane with his shoe, but now we are scared that someone might.

Another part of Information Warfare that affects us daily is hacker warfare. Look at the SANS institute. Do you think there would be SANS if there wasn't Information Warfare or more specifically Hacker Warfare? We can look at CERT statistics to see how active Hacker Warfare has been this year. So far there have been over 73,000 reported incidents to the CERT® Coordination Center (CERT). Imagine how many incidents went unreported or undetected! I realize not all of the incidents reported are hacker warfare as we have defined it, but even if 25% are, that's still over 18,000. The other areas of Information Warfare as discussed in this paper are probably less likely to affect us on a day to day basis like Hacker Warfare and Psychological Warfare do, but that doesn't mean they couldn't. The key to protecting yourself against Information Warfare is to

have a solid knowledge of and practice good OPSEC and INFOSEC procedures while having a corporate contingency plan to counter any attack.

Conclusion

The world is a rapidly changing place, and Information Warfare is playing a big part whether we recognize it or not. It's important to understand each of the areas of Information Warfare as a security professional. I've shown Information Warfare includes more than Hacker Warfare and I am positive as technology grows so will Information Warfare. Currently, Hacker Warfare might be the area of Information Warfare you are most familiar with, but as you have read, all the areas of Information Warfare are critical to our daily routine in our personal and professional lives.

References

Libicki, Martin. "What is Information Warfare?" URL: http://www.ndu.edu/inss/actpubs/act003/a003ch03.html (4 Jan. 03).

Department of Defense. "Dictionary of Military and associate terms." Joint Pub 1-02 URL:http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (4 Jan. 03).

Department of Defense. "Joint Doctrine for Information Operations." Joint Pub 3-13 URL:http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (4 Jan 03).

Lewis, Brian C. "Information Warfare."
URL: http://www.fas.org/irp/eprint/snyder/infowarfare.htm (4 Jan 03).

Goldberg, Dr. Ivan K. "Information Warfare." Glossary of IW Terms.
URL: http://www.psycom.net/iwar.2.html (4 Jan 03).

Space and Electronic Warfare Lexicon. "Electronic Warfare." Glossary E.
URL: http://www.sew-lexicon.com/gloss_e.htm#ELECTRONIC_WARFARE (4 Jan 03).

Institute for Telecommunication Sciences (ITS). "Operations Security".
URL:http://www.its.bldrdoc.gov/fs-1037/dir-025/_3695.htm (4 Jan 03).

Schiffman, Betsy. "Stolen Qualcomm Laptop Contains Sensitive Data."
Forbes.com. URL: http://www.forbes.com/2000/09/19/mu5.html (4 Jan 03).

Psywarrior. "Psychological Operations."
URL: http://www.pipeline.com/~psywarrior/ (4 Jan 03).
URL: http://www.psywarrior.com/ec130.html (4 Jan 03).

Checkpoint. " "Solo" tells Afghans they are not alone." Operation Enduring Freedom.
URL: http://www.checkpoint-online.ch/CheckPoint/J3/J3-0007-AfghanistanUSPsyOp.html (4 Jan 03).

Heng, Li. "Chinese, US hackers fought all out." People's Daily.
URL: http://english.peopledaily.com.cn/200105/16/eng20010516_70123.html (4 Jan 03).

CERT. "CERT/CC Statistics 1988-2002." CERT Coordination Center.
URL: http://www.cert.org/stats/cert_stats.html (4 Jan 03).