Global Information Assurance Certification Paper

Information Warfare:
Are you battlefield ready?

Phillip A. Conrad

What is Information Warfare and why should I care about it?

> *Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary.*[1]

Winn Schwartau gives the best definition I have found for Information Warfare (IW). Add to this the three different classes of "personal IW", "corporate IW", and "global IW". Let's take a look at these three classes and see why they are important to all of us.

Personal IW can take many forms at the same time or one at a time. Types of "personal IW" can range from a bad credit report to a major phone system outage. What if you went to the store and paid for your items with a credit card, only to find out your card was rejected? No big deal, or is it? You may have just missed a payment, or you may be the victim of identity theft. You could be the target of a "personal IW" attack, someone trying to destroy your credit. Any information about you that is stored or used electronically is vulnerable to attack.

Corporate IW also takes many forms. Corporate IW is an attack on what your company uses day to day to maintain its business. Therefore, anything from phones to electronic funds transfer are targets of IW. In January of 1998 there was an outage of a major phone system in Frankfurt.[2] Approximately 54,000 phone lines were affected. Most lines were down for two days, but full restoration took ten days. Now, if your business were affected that way, could you afford to be without phones for ten days? What if this was not an accident or equipment failure, but rather a directed attack by an Information Warrior? What if this happened to more than one switching station at the same time? Would your company be able to withstand this kind of attack? Recent attacks have taken a more subtle form. When was the last your company had to deal with an e-mail virus? "*A flood of e-mail messages originating in Australia and Estonia – and routed through the White House computer system – virtually shut down Langley air base's e-mail for hours.*"[3] If this could happen to a government computer system, imagine what it could do to a small or large business's computer system. Everything that you use in this manner must be protected. Corporate resources are the most likely to be attacked.

Global IW has the potential to be the most devastating of any type of IW. Think what would happen if someone was able to take control of the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the main system for international interbank funds transfer.[4] Banks and/or entire nations could go bankrupt in a matter of hours. You could defeat your enemy without ever setting foot on their soil or even firing a shot. A bloodless war where everyone is the victim. Then there are the communications satellites that orbit the earth. Those could be used for many types of

propaganda attacks. Currently, attacks of a personal or corporate nature can come from anywhere on the globe via use of the internet. This makes IW the weapon of choice for a small nation or terrorist group and the internet as the delivery platform.

Where is the battlefield and am I on it?

The battlefield of IW is all around us and we never really pay attention to what we see. Every day someone is waging war on the battlefield. Sometimes we see it, and sometimes we never know what is happening. The more you look, the better you will be able to see the signs of the ongoing battles.

The battlefield for personal IW is varied and sometime difficult to describe. This includes such things a credit cards, cell phones, and e-mail on personal computers. Any personal information that is kept about you by someone other than yourself could be considered part of the battlefield. This kind of information includes such things as insurance companies, doctors offices and hospitals, the IRS, the Social Security Administration, state license bureaus , phone companies, and credit card companies. Although most people are not on the front lines of the battle, almost everyone is on the battlefield. Every time you connect your personal computer to the internet, you are on the battlefield and are vulnerable to attack. Every time you use a credit card, a cell phone, or an ATM, you are making your personal information vulnerable to attack. Does this mean that every time you use your credit card you are going to be attacked? No, most likely not. However, every time you connect your personal computer to the internet, you are subject to attack from people, companies or governments from anywhere on the globe. The longer you stay connected, the higher the risk of being attacked. What it all comes down to is this: Any personal information about you is your personal IW battlefield.

The battlefield for corporate IW is somewhat easier to define. This would be your company facility and all its computer systems. It could also include your company's bank and any other companies that supply parts to your company. In this world of "just in time" parts, would an attack on a parts company be an attack against them, or against your company? Every time your company connects to the internet, they are vulnerable just like your personal computer. If your company has a dedicated full time connection, then you are on the battlefield 24 hours a day. Most likely you are even on the front lines of the battlefield. Every time you send or receive e-mail you run the risk of a computer virus infection. This alone could cripple a company. Then there are the phone lines, electric suppliers, and so on. Anything that you need to keep your business running is part of the battlefield and subject to attack at any time. Still think that you are not on the front lines of the battlefield?

When it comes to global IW, everyone is on the battlefield. Global IW has the potential to do the most harm. It is warfare on a global scale. Every hi-tech site on the globe is a potential target for global IW. By using the internet every major city can be reached from almost any place on the globe in a matter of seconds. It is frightening to think that someone with a wireless cell phone could send off a signal that could start an attack leading to the collapse of an entire country on the other side of the globe. There have been reports as early as 1991 that site the KGB and Cuba were developing computer viruses to launch at the United States and NATO.[5] Although there have not yet been any

reported acts of global IW, it is only a matter of time before it does happen. The only people able to escape a global IW attack would be the ones with NO technology.

How can I prepare for battle?

There are many ways to prepare for the three types of IW. The type IW you are preparing for determines how much and what you can do. Sometimes being over-prepared can be worse than under-prepared. The best thing is to test the procedures that you have put in place to deal with an IW attack.

How can you protect yourself from a personal IW attack? It is not easy. In our current society there is no way to be completely secure. There are, however, many things you can do to help protect yourself. Do **not** give out any personal information to people or companies that do not have a need for that information. Be careful when using credit cards, calling cards and cell phones. Do not give out your Social Security Number to anyone except your employer. Make sure to shred any papers that have financial or personal information on them before discarding them. Put an anti-virus program on your personal computer to protect you from program attacks and install a personal fire wall program to protect your computer from outside attacks. Do not share ANY of your computer files to the outside world. If you have any sensitive information about you on your computer, make sure that you use a password to access the computer and/or files. Make backups of your computer files often, in case they are destroyed accidentally or on purpose. Remember that any e-mail you send is **not** private and could be read by anyone along the route to its destination.

Protection against corporate IW can be a very monumental task. The SANS Institute's Joint Computer Security Conference, held January 2001, included topics to deal with this subject. In theory, a well-funded, organized attack could send the target society into chaos. The results of an informal poll of companies indicated that 17 percent were prepared to respond to a corporate IW attack.[6] Indications are this is a time consuming and expensive task to fully prepare for an IW attack. It is for this reason that more companies should be aware of what is required to prepare and start to take steps to accomplish this. If a company is not prepared for an attack, then it is most likely to be crippled by such an attack. Going into great detail on this subject is beyond the scope of this paper, however, it is important to note several highlights. You should have physical security for your business. Next you should secure the computer system/network on the inside. Make sure that only the people that need access, get access. Then secure your computers/networks from the outside making sure that no one can get into your computers that is not supposed to. This is the hardest task to perform because as you block one way in, someone finds another way in. Protection against a corporate IW attack may be the most important and the most difficult to perform.

Defending against a global IW attack should be no more difficult than defending against a corporate IW attack. The biggest problem with a global IW attack is that you as a person or you as a company may only be a small part of an attack. Who is responsible for determining the scope and breadth of the attack? The military has the experience and the infrastructure to deal with such attacks. However, if the attack is not against a military site, there is nothing they can do.[7] This means that the civilian sector must find a

way to coordinate things. Robert D. Steele believes the Department of Defense (DoD) must lead the way in dealing with IW attacks and the corporate world must learn the military way of thinking when it comes to dealing with IW.[8] Once there is a way to coordinate all the information about a global attack, the next thing to deal with is any kind of counter attack and/or prosecution of the offending parties. This will be the most difficult task to perform, with its own set of problems. So far there are no international laws or treaties that deal with IW attacks. Crossing international borders is not the same as crossing state lines. Launching a counter-attack could start an international war in the real world instead of the information world. These and many more issues must be considered before we can say that we are ready for a global IW attack. We must be prepared for an IW attack that most experts say is only a few years away.

So, are you battlefield ready? You should be by now. If everyone is battlefield ready in the personal and corporate arena, then it might be possible to delay or prevent a global IW attack. You are always on the battlefield in one way or another, so always be prepared.

---

[1] Schwartau, Winn, "Information warfare: cyberterrorism: protecting your personal security in the electronic age / Winn Schwartau." 1994,1996

[2] Church, William (editor), "CIWARS Intelligence Report 25 October 1998". 28 Oct 1998. URL: http://www.infowar.com/resource/resource_102898a_j.shtml

[3] Rothberg, Donald M. "Cyber Warfare". 08 Oct 1997. URL: http://www.infowar.com/civil_de/civil_de_100897a.html-ssi

[4] Brown, Cadet Edward J, USAFA. "Information Warfare and Finance: A Strategic Target". Dec 1996. URL: http://www.infowar.com/civil_de/Pol499c.doc

[5] Meeks, Brock N., MSNBC "Information warfare and the real threat. Government should use caution in responding to foreign info-threats".04 Jan 1998. URL: http://www.infowar.com/civil_de/civil_de_010498b.html-ssi

[6] Radcliff, Deborah "InfoWar Games". 22 Jan 2001. URL: http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO56588-,00.html

[7] Radcliff.

[8] Steele, Robert D. "Information Peackeeping: The Purest Form of War" URL: http://www.oss.net/InfoPeace/

Last Updated: March 21st, 2018

Upcoming Training

SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 03, 2018 - Apr 08, 2018	vLive
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201804,	Apr 09, 2018 - May 16, 2018	vLive
Community SANS Charleston SEC401	Charleston, SC	Apr 09, 2018 - Apr 14, 2018	Community SANS
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, Switzerland	Apr 16, 2018 - Apr 21, 2018	Live Event
Mentor Session - AW SEC401	Memphis, TN	Apr 17, 2018 - May 17, 2018	Mentor
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS Riyadh April 2018	Riyadh, Saudi Arabia	Apr 28, 2018 - May 03, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, IL	May 01, 2018 - May 08, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
University of North Carolina - SEC401: Security Essentials Bootcamp Style	Charlotte, NC	May 21, 2018 - May 26, 2018	vLive
SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
Community SANS New York SEC401	New York, NY	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event