Global Information Assurance Certification Paper

A Short Trek Through the Theory of Information Warfare

E-Warfare Certification (GEWF)
Practical Assignment
Version Number v1.0
Assignment Option 1: Research

Joseph L. Cosgriff
E-Warfare / Las Vegas, NV / September 2005

Table of Contents

Abstract

This paper was written with the intent of providing not only the academic side of Information Warfare (IW) but also general "practical use" supporting information. Put together somewhat like an historical study of the concept, it begins with a "what is IW" and then moves to a short story written to assist the reader in further understanding the theory of IW. From this point, the paper explains the modern battlefield and the advances that have taken place.

After a brief explanation of the OODA Loop, the paper explains the progression of warfare in general and it's driving forces. The paper finishes with the "practical use" application side of the discussion. Topics such as who is the threat and what should be done are briefly explained.

While I don't profess to be any type of expert in this subject I do feel that my understanding of the topic is sufficiently outlined in this paper. I support the information with years of experience in the area of information assurance and information warfare.

Joseph L. Cosgriff What is Information Warfare (IW)?

Warfare as a concept and in an operational perspective has been around since the first time man or groups of men decided to gain an advantage over another man or men. Whether we are talking about the singular concept of battle waged between two individuals or the large-scale operations conducted by countries, at their core there are basic concepts or strategies that must be employed to succeed.

One of these concepts or strategies is that of Information Warfare (IW). It is a part of war that has proven it's self most valuable. The organization that takes advantage of gained information and uses that information will many times be victorious. The converse to that is the organization that fails in it's attempt to capitalize on information and/or fails to engage in operations that enhance their own IW capabilities.

Whether we are talking about Psychological Operations (PYSOPS) or cyber offensive and defensive methods of battle, the goal should be the same. Assess what you know, determine gaps in that knowledge, develop methods to gather or provide information to address those gaps, implement operations that utilize the "gained" information, and then start the process over again, and again, and again…

In a report for Congress written by Clay Wilson [1] (a Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division), he writes that the Department of Defense (DOD) views (from a technical perspective) IW as information, "that… is now a realm, a weapon, and a target." It is part of the Battle Field (military or business) environment.

All military leaders, military intelligence analysts, and civilian business C level personnel, should understand that fighting in the arena of IW requires new view points. The definition of IW is not restricted to "electronic" type data. It encompasses many aspects of information and the methods and means in which to access, gather, alter, and disseminate information.

While the definition outlined above referenced document does show the broad ways in which IW can be directed. It also proves that the winds-of-change are blowing. The gap of understanding about cyber related IW is reduced with each new group of leaders that graduate from a military academy or business leaders that assume the role of "Commander-in-Chief" of some American company.

Joseph L. Cosgriff A short story of Information Warfare

In a room filled with about two-dozen computers there sits a high-ranking US military officer at a desk with three monitors. The officer's desk is perched on a raised platform higher than the other desks in the room. From this vantage point and with the officer's monitors, he can scrutinize, direct, and view everything that happens in the room as well as switch the views on his monitors with the teams and ongoing operations located below on the floor.

The room is in the shape of a half circle. On the walls against the curved side of the room there hangs large screen monitors that run from about eye level to about 20 feet above the floor. Each monitor (probably 15 or so) presents information back to the viewers in many different formats. Some are actual live "feeds" while others are depicting actions that are happening and being directed by operatives sitting in the room.

The teams located on the floor represent a subsection of military units deployed around the world. Some of the members are assigned to regular military units while some are assigned to very secretive and clandestine detachments.

The room is located in an underground bunker to protect the equipment from physical attacks. There is one door to this Tactical Operations Center (TOC) and each officer entering or exiting must offer an eye and hand for positive biometric identification. Even with these measures, outside the door sits an armed military police officer guarding against other intruders.

At the present moment the high-ranking military officer is watching one of his teams engaged in a fierce battle with a terrorist group. This battle while to the outsider may seem unimportant, is actually being conducted to save lives and minimize damage to facilities. There are short spurts of attacks and countermeasures. Teams operating in conjunction with each other teams to out maneuver and out think an enemy who is not bound by political and/or military codes of conduct.

At one point in the battle the US operators obtain information that could prove vital if acted upon immediately. With communication lines directly to key leaders within the Theater of Operation (TO), decisions are made and actions taken. The speed in which the US operators acted on the "gained" information allows them to defeat the enemy in this single but important battle. "YEA! ALRIGHT!" sounds out throughout the TOC. The operators were successful and they have beating an enemy that didn't play by the rules.

While the short-lived celebrations are played out on one side of the TOC with that one team, other teams are feverously continuing to fight and win (and in some instances lose). The high-ranking officer just sits back and contemplates his wins and loses today. He understands his troops need to show positive

emotional exuberance after successful operations. However, he also understands that when any operation is complete there is damage that must be repaired. There are “lessons learned” and “after action reviews” that must be conducted to see how the overall success or failure is addressed.

This short story, while fictitious to my knowledge, was added this report to show the changing ways in which the US military and other countries will and are possibly fighting their battles today. It doesn’t matter where the solider, sailor, airman, or marine sits today. At some point they use information to fight and win a war.

This could be real world or it could be a very sophisticated war game designed to strengthen the skills of the military officers that could be involved in such operations. Regardless it must be addressed and integrated into current and future training methods.

One example of this integrated training into future operations is with the United States Marine Corps (USMC). As part of the Title X Wargaming, [2] the USMC integrates IW and Critical Infrastructure training programs as part of the over all concept. Under the “Revolution in Military Affairs (RMA) Series,” they address a wide range of issues to include “an extensive Information Warfare (IW) effort.”

Joseph L. Cosgriff What's on the modern battlefield?

On the modern battlefield today, computers are everywhere. Compared to 20 years ago the computing power in a military unit today is almost unbelievable. One could almost make an analogy with the difference between an American Revolution era battle ship and a US Naval vessel of today. Whether it is 200 years of battleship advances or 20 years of information system advances the modern battlefield is filled with equipment that effects IW operations.

During Operation Iraqi Freedom (3rd rotation – OIF3) there were computers on almost every work desk. Soldiers had access to classified email systems with one system as well as unclassified DOD provided email systems. There were Internet cafes in base camps throughout the country.

The modern solider today can send an email to a loved one in the morning before they report for duty. Conduct a military battlefield operation in the afternoon. Then in the early hours of the evening, sit down and manage their bills and conduct online banking, all with no impact to military readiness.

There is an understanding with military leaders that the mission comes first but the soldiers come always. This means that all things being equal, the mission is the priority. But to accomplish the mission, soldiers are needed. With this understanding, leaders allowed soldiers the ability to communicate regularly with family and friends.

Families could stay in touch through online chats (Instant Messaging) and web cams. While good-old-home-cooked cookies was still a delight from the US Mail system the need for old fashion letter writing has almost go by the wayside. The other methods of communications allowed for a wider use of information systems.

However, with this utilization of so many information systems, came the need for an increase in Operation Security (OPSEC). As the saying goes, "make a better mouse trap…" well make information systems easier for people to use and have access to and you will have people beat down the preverbal door of security to gain access to it. Thereby making the job or protecting IW systems from information leakage.

It doesn't take a PHD for someone to see that with all those systems within the environment it requires extreme due diligence on the part of the Information Assurance officers to ensure they stay protected.

Old fashion anti-virus software, firewalls, and training classes go far in the campaign of IW.

Joseph L. Cosgriff The Learning curve (The OODA Loop)

There are a number of issues with training IW soldiers. Of those issues, the critical "timing" nature of acting on information obtained is of vital importance. When, as depicted in the short story of this report, one organization acts quickly and within the parameters of an educated decision making process they stand a higher percentage of success.

The concept of the "OODA Loop" (Observation, Orientation, Decision, Action) shows how this can be accomplished and reinforces the need for quick and timely decisions. Originally developed by Col John R. Boyd, USAF (Ret) to teach fighter pilots how to out maneuver their enemy, it can be applied to almost any concept when one element gaining a "tactical" advantage over another element is important. That can be related to military or business operations.

In the US Army, Military Intelligence Analysts are taught to observe (the first O in the OODA Loop) actions on the battlefield and search for indicators. These indicators allow them to, with some degree of certainty, use predictive analysis when addressing an enemy threat. Once they have discovered these indicators they move to the second phase of the decision making process.

They second phase is the orientation phase (the second O in the OODA Loop). During this phase, the analyst assesses the indicators validity to the current operation. They use historical information to process assessments. One part of this in the current war on terrorism is the concept of "Atmospherics." The term, while deriving its origin from the study of the atmosphere (weather related), actually is a concept of attempting to gauge the current environment (the local populations view point) within a cultural to determine potential hot spots or issues and concerns.

After a proper assessment has been conducted or the observation has been oriented to what is happening at that time a decision must be made (the D in the OODA Loop). Words such as timely and effectively come to mind during this phase. All the information in the world is useless unless acted upon and acted upon quickly. But even with that, if the decision made is not made with a certain level of certainty and understanding of the environment, it may be fruitless.

Once the decision has been made and the course of action has been determined it must be acted upon (the A in the OODA Loop). As stated above, you can understand what is happening, you can have the right course of action, but if you don't act… you lose!

So, it doesn't matter if you are a fighter pilot jock, a military intelligence analyst or the information security manager for a large fortune 500 company, the OODA loop is a tool that you can use (and if used properly) to assist you in defending and defeating an enemy.

History repeats it's self…

If Fourth Generation Warfare had to be summed up in one statement, the above statement would probably be the most appropriate. After the Treaty of Wesphalia in 1648, the primary organization that assumed responsibility for conducting military operations became the state.

The Treaty of Wesphalia was a treaty that allowed a group of European settlements, to negotiate peace and establish some level of excepted protocol between the delegated territories[3].

The below diagram depicts (graphically) the concepts and phases of the excepted generations of warfare as explained in an article by William S. Lind, "The Canon and the Four Generations," dated June 11, 2004[4].

The graph summarizes Mr. Lind's description of the phases, general time frames, and some of the driving forces or catalysts for the major changes. It is provided to allow for a quick understanding of the progression in generation of warfare.

Which Generation of Warfare	Prior to the establishment of the Generation of war	First Generation	Second Generation	Third Generation	Fourth Generation
Time Frame	Pre-1648	~1648	~1918	~1918	Depends
Driving Force	War was waged by individuals or groups; Different entities conducted operations based on need or desire.	End of "Thirty Year War"; States assume responsibility to wage war.	Firepower & Attrition warfare; "The artillery conquers, the infantry occupies."	Maneuver warfare; Developed by Germany; the Blitzkrieg.	Marks the end of the state's monopoly on war; Different entities are fighting wars.

Diagram 1: The Generations of Warfare

As depicted above, it is easy to see how the statement that started this section fits appropriately. The current worldly environment from a purely military standpoint shows how we have progressed or digressed depending on your view point to a time before 1648. For over 350 years we have developed concepts and strategies to conduct warfare, which has changed. It will continue to change as our dependencies and development of information systems

continue.

The phrase, “it is all relative” fits nicely in this section. Mainly because, depending on your line of work, what you do and whom you do it for, threats relating to IW can come in many forms. For a company that develops “next generation” military equipment, your threat can be foreign governments, competitors or domestic terrorist groups if your development disrupts some natural resource.

If you are a private company that makes widgets your threat can be from your major (or minor) competitor. You could be attacked by methods such as social engineering (for possible data mining operations) or deliberate and outright cyber directed attacks. Any company worth their weight stocks should, in these modern times of multiple avenues of ingress and egress points of a network, not only acknowledge the potential for these actions but should also work towards addressing them in some form or fashion.

With large military oriented operations, the threat can be from the observed or “silent” enemy. Attacking and directing IW operations to meet a military objective is as important as a traditional “Force-on-Force” operation. As the development of technical means for communications increases the means in which we utilize and protect that means increases as well.

Cyber attacks, physical attacks or IW concepts are all driven by someone for some reason. They interrelated and interconnect at some level. In a report (dated September 22, 2001) from the Institute for Security Technology Studies at Dartmouth College, titled – “Cyber Attacks During The War On Terrorism: A Predictive Analysis,” it was reported that cyber attacks accompany physical attacks almost immediately.

> “Subsequent to the April 1, 2001 mid-air collision between an American surveillance plane and a Chinese fighter aircraft, Chinese hacker groups immediately organized a massive and sustained week-long campaign to cyber attacks against American targets.” (5)

The answer to this sections title question, “Who is the threat?” is only as relevant as the entity in which you are speaking of. The threat of one organization can be the threat to another or not. Who your threat is, depends on what you do and how you do it. Assessing that information and determining your vulnerability to threats allows you to develop a clearer picture for “who the threat” is.

Joseph L. Cosgriff What needs to be protected (Business vs. Military)?

The plethora of items that must be protected are as diverse as the possible entities that must protect the information. Regardless of whether your enemy is a battle hardened veteran or a ruthless business competitor every individual responsible for the protection of information must understand IW and deal with it.

While lives are not necessarily lost during business operations, even during a hostile take over, it is still important to understand the concepts of IW. Some of the same steps that military leaders take to assess an enemy are taken by business leaders.

For this paper, the information talked about for protection is the information that would be considered most dangerous to an organization if leaked. In the military, they usually identify courses-of-action that address three primary avenues. They are, most probable, most likely, and most dangerous.

While two of them (likely and probably) may sound similar, they are different. In some instances they may be synonymous. However, what may be probably is not necessarily likely. Depending on the evaluated threat (threat assessment), one potential course-of-action may be very likely but not probable.

The most dangerous course-of-action is the enemy avenue that, if acted upon, could cause the most significant impact to an operation. Usually, from a military standpoint, the most dangerous is not necessarily likely or probable. If, proper steps have been taken to protect and defend against such actions.

This brings us back to the understanding of the OODA Loop. As an operation progresses, regardless of military or civilian, more information is obtained. As it is obtained, is should be evaluated and acted upon.

To put it another way, let's say that an information security managers has just assessed the operations at her data center. She may outline in a document what an enemy (using the term very loosely) may do to gain information that is stored or processed through the data center.

Separate courses-of-action may be outlined and documented with countermeasures or protective measures put in place. She may document that the most dangerous thing that could happen (speaking strictly from an industrial espionage standpoint for ease of explanation) would be that an aggressive competitor could have someone break into the data center to steal the data from a restricted server that contains the product information for a brand new widget.

While highly unlikely because she has motion sensors and armed guards at the gate of the facility, it is still a consideration that she must take into account.

So, how do we protect our critical infrastructure? What measures must be taken to ensure we don't lose the battle or the competitive edge?

We must first attempt to thwart or deter IW types of attacks. Depending on what aspect of business or military operations we are talking about we must include elements from all aspects and levels.

For example, in the business world, the data center manager cannot control or manage the entire networking environment. This manager must work cross functionally with other business groups to ensure information assurance systems are properly assessed, developed and implemented. Administrative functions such as training and proper employee hiring procedures must be followed.

System Administrator operations must be properly documented and audited to ensure compliance. Information Security Managers must continually assess external as well as internal threats related to IW so that policies and procedures can be reviewed and updated to ensure current applicability.

The utilization of off-the-shelf or open-source security products should used so that sufficient information can be gathered that allows for proper distribution of reactive and proactive IW systems. If not possible then home-grown solutions, at a minimum, must be employed.

The Military service member fighting the IW battle everyday must understand that constant training and research to address emerging technologies and applications must be done continuously. The new generation of warfare requires a new generation of warrior. While there will always be tactical battles that are won and lost, the ability to use information in the realm of IW is vital.

The concept of using IW as a weapon or targeting it for military strategic advantage must continue to progress. Continuous review of current operational requirements and developments must also take a higher priority if the US is to maintain it's current place as a world power.

Joseph L. Cosgriff References

(1) Wilson, Clay; Information Warfare and Cyberwar: Capabilities and Related Policy Issues; July 19, 2004. Congressional Research Service, The Library of Congress. http://www.au.af.mil/au/awc/awcgate/crs/rl31787.pdf

(2) Title X Wargaming, USMC. http://www.mcwl.quantico.usmc.mil/ecp/4-Wargaming/ECP-Wargaming%2022%20Dec%2004.pdf

(3) Encylopedia Britannica 2002, Expanded Edition DVD; http://www.hfac.uh.edu/gbrown/philosophers/leibniz/BritannicaPages/WestphaliaTreaty/WestphaliaTreaty.html

(4) Lind, William S., The Canon and the Four Generations; Antiwar.com; June 11, 2004. http://www.antiwar.com/lind/?articleid=2791

(5) Vatis, Michael A.; Cyber Attacks During The War On Terrorism: A Predictive Analysis; September 22, 2001. http://www.ists.dartmouth.edu/library/analysis/cyber_a1.pdf

Diagrams

Diagram 1: (page 9) The Generation of Warfare. Cosgriff, Joseph L. (note: This diagram was developed by myself with extracted information from the reference #4 listed above.)