Strike Back: Offensive Actions in Information Warfare

Donald J. Welch, Nathan Buchheit, and Anthony Ruocco
Department of Electrical Engineering and Computer Science
United States Military Academy
West Point, New York 10996

Introduction

This paper is written in the context of Information Warfare being a serious and direct threat to our nation's security. The National Security Council defines such threats as ones that endanger our national goals and objectives. In general, these include threats to the lives of American citizens and residents, threats to our economy, and threats to our ability to promulgate freedom, liberty, and the rule of law to the world. It is in our national interest to stop a terrorist organization from bombing the World Trade Center. It is equally important to our national interest to prevent Information Warriors from shutting down or threatening our essential financial, health, or quality of life infrastructures. Winn Schartau, as well as many others, has made the point that Information War threatens our national security every bit as much as conventional war [14]. We will not restate those arguments here but proceed with the assumption that they are true. This paper then, represents a thought experiment on a grand scale.

What we propose is considered by many to be a drastic departure from present policy and law.[1] We readily acknowledge that certain laws and policy would have to be changed in order to implement some proposed actions necessary to meet the threat of Information Warfare. We do not advocate or recommend that action be taken based upon the suggestions contained herein until such time as our nation's policy and laws do change. We are not advocating or recommending any illegal action. We are recommending reconsideration of the laws and policies such that we are not restricted to fighting a "no-win" war.

Defensive Wars Are Not Winnable

History has demonstrated that military conflict, whether conventional or unconventional, requires several elements for success. Foremost is a clear definition of victory in order to guide efforts and achieve success. Additionally, we must recognize the fact that the combatant who does not seize the initiative from the enemy through offensive actions is doomed to defeat.

In order to achieve victory we must first understand our national goals and then determine what means we have that allow us to attain them. We then identify what capabilities the enemy has of defeating us, thus thwarting our national goals. Information war also requires a clear understanding of the national goals. And in fact, a distinguishable definition of victory becomes even more vital to success in information warfare since it more closely resembles a war against terrorists, i.e. unconventional warfare, knowing enemy strengths and weaknesses than a war of armies clashing on the battlefield.

In strategic terms this is referred to as identifying the enemy's *Center of Gravity*. For example, the goal of the Persian Gulf War was the liberation of Kuwait. U.S. planners correctly determined that the Iraqi Center of Gravity was the Republican Guard element of the Iraqi army. When the Iraqi Republican Guard was decisively defeated, it withdrew from Kuwait. A correct understanding of an opponent's center of gravity is one of the most difficult requirements of a successful strategy. Many campaigns and wars have been lost because the losing combatant did not identify the winner's true center of gravity.

The need to strike a decisive blow to the enemy's center of gravity in order to achieve victory highlight the futility of engaging in only a defensive war. Save the convergence of extreme circumstances and ineptitude on the part of an adversary, assuming a purely defensive posture tends to result in the aggressor emerging victorious. Two examples from this century are the French at the start of World War II and our own experience in the Vietnam War.

One of the lessons the French learned from World War I was that they had to defend their soil from the Germans. They spent a huge amount of money, effort, and time on the construction of the Maginot Line. This series of interconnected defenses employed the best defensive technology of the day. Hardened fortifications that were mutually supporting. Defenses arranged in depth. Obstacles covered by fire. The Maginot Line was virtually impenetrable. The Germans, however, had learned different lessons from World War I. The German studied the French defenses and when ready, choose the time, place and nature of the battle. They had the time to find the French weaknesses, decide how to best exploit those weaknesses, and prepare for the battle without interference. They made

[1] The ideas expressed in this paper are strictly the ideas and thoughts of the authors and in no way represent the official position of the Army of the United States or any other official government agency or organization.

limited use of the best offensive technology, employed tactics and strategy that emphasized the offensive and with the least mechanized army in Europe defeated France in about two weeks.

A very different type of conflict that also failed because of an improper employment of offensive strategy was the U.S. involvement in the Vietnam War. The U.S. Army never lost a major battle during the conflict and yet lost the war. In its attempts to limit the war and prevent escalation, the U.S. elected to fight a defensive war to protect the Republic of South Vietnam from the Viet Cong insurgency and North Vietnamese Army. Limited attempts were made to strike at the heart of the North Vietnam war effort through aerial bombardment. The North Vietnamese Army and Viet Cong could choose the time and place for major battles and then escape across the border before the U.S. could inflict a decisive defeat. Meanwhile the key factor in the U.S. war effort - public support - was dealt blow after blow, eventually forcing the capitulation of the U.S. It took a tremendous expenditure of resources (time, money and manpower) for Vietnam to break the U.S. public's will to support the fight i.e. our center of gravity. In contrast, the U.S. chose not to strike at North Vietnam's center of gravity and instead fought a mostly strategically defensive war. The U.S., by meeting the attackers on the attackers terms, never forced North Vietnam to defend itself. This gave the North Vietnamese time to build up to a fatal blow to the U.S. center of gravity. And although wars are complex and these examples simple, history has shown us the folly of trying to fight a defensive war time and again.

Making a leap from pillboxes in France or the jungles of Vietnam to the complex world of cyberspace may seem extreme to some. But in actuality it is not as far as one might first think. Maintaining a completely secure network is an extraordinarily time-consuming and difficult task. Keeping up with patches and fixes is a tedious and thankless task. The reliance on patches provided by vendors means that a network will always have a window of vulnerability between the time the problem is discovered and the time that the fix is designed, built, tested and fielded. A determined attacker will eventually discover a vulnerability before the patch is installed. Much like the commando who can wait all night for a sentry to be distracted for just a second, the patient Information Warrior will eventually be rewarded. Fred Cohen has made the case that sitting back and waiting for attackers is a strategy doomed to failure [13].

Much as the Germans were able to wait for the right opportunity and attack where the French were weak, an information attacker only needs to overcome the weakest defenses in the network to win. Similarly, the Information Warrior attacks and because he too selects the time and place he can focus all his energy and resources to overcome the defense's weaknesses. Information warriors have time on their side just like the North Vietnamese did. Defending against every possible attack is resource intensive and fraught with human error. Between the World Wars Douhet said, "The bomber will always get through" [12]. His point was that it was a big sky and it was impossible to find and stop every bomber. An appropriate paraphrase for the cyber-age is "The Information Warrior will always get through."

Fighting an Information War offensively does not necessarily mean that we must assume the role of the aggressor. In fact, being the aggressor does not always guarantee victory. But fighting a strictly defensive war, one fought by meeting the enemy at the place and time of the enemy's choosing practically guarantees defeat. A rational enemy will only fight when the chances of success are in his favor. Allowing the enemy to always hold the initiative and only reacting to his efforts is fighting defensively.

Fighting an Information War offensively does mean maintaining a strong defense and then, at the proper time, grabbing the initiative from the enemy, defeating him when and where he is weakest. This necessary integration of an offensive characteristic into the defense also helps assure that a decisive battle will be engaged with the enemy. This is in contrast to a strictly defensive posture, which often creates a situation in which a decisive battle is never fought

A decisive battle can be defined as a battle that destroys the enemy's center of gravity, and hence his ability to fight. On the conventional battlefield our goal is to engage the enemy in such a battle, fight it on our terms and by winning, stop the enemy'sability to conduct operations against us. That is the only way to win. Defensive battles are fought only as a stopgap measure. They are a means of preventing the enemy from decisively destroying us before we are able to maneuver him into decisive battle on our terms.

The concepts are the same in Information War, only the application is different. Before we can fight a decisive battle, we have to correctly determine the enemy's center of gravity. Then we can attack that center of gravity leaving the enemy incapable of conducting cyber-operations against us. It is acknowledged that determining the correct center of gravity in Information Warfare is not a trivial task. Below we define a taxonomy of potential enemies and a representative list of their potential centers of gravity.

Category	Description	Potential Center of Gravity
Crackers	Small loosely organized groups with personal satisfaction a primary goal	Personal freedom, personal wealth, access to computing infrastructure
Criminals	Small loosely organized groups with personal wealth the primary goal	Personal freedom, personal wealth
Organized Crime	Organizations with the resources whose ultimate goal is wealth	Wealth, obscurity, knowledge of adversaries, secrecy

Terrorists	Organizations whose primary goal is political	Secure support and operating areas, target intelligence, obscurity
Corporations	Organizations with a legitimate primary purpose who wish to enhance their success through information warfare	Secrecy, knowledge, wealth
Friendly Governments	Governments friendly to the U.S. in other areas who wish to gain, economically, militarily, or politically from Information Warfare	Secrecy, knowledge, finance, information infrastructure
Enemy Governments	Governments not friendly to the U.S. who may have the same goals as Friendly Governments but also wish the U.S. ill	Knowledge, finance, information infrastructure

This is an admittedly general list since the classification of an entity into a specific category is a formidable task and the delineation of categories is open to debate. However, this list provides a starting point for discussion on the possible centers of gravity that Information Warfare adversaries may have.

Starting with the simplest example, a cracker will not be able to cause much trouble if incarcerated. Therefore, the center of gravity in this instance may be personal freedom. Striking at a cracker's personal freedom may not be easy and may take many different forms. In some cases just threatening it may be enough to cause a cracker to stop attacks. For example should our adversary be a cracker residing in the U.S. we could strike at personal freedom by collecting criminal evidence and turning it over to the Federal Bureau of Investigation. A cracker that resides in a hostile country would, in all probability, have to be attacked in a different manner. It is unlikely that the Iranian police would be willing to prosecute and incarcerate an Iranian national who breaks into U.S. Army computers. However, having the capability to plant evidence, which implicates the hacker of being guilty of an unrelated crime, might get the Iranians to accomplish our goal for us.

The higher an adversary is in the taxonomy, the more potent the threat to national security. A foreign corporation that competes with U.S. corporations may try to steal critical information or compromise information that the U.S. corporation already owns. Should that foreign corporation be from a country that has strict and enforceable laws their center of gravity may be secrecy. Should they be from a rogue country, exposure may have little consequence. However, they may have information assets of their own that are key to their survival. This corporation may rely on foreign investment or other aspects of finance that can be manipulated. Degradation of their ability to conduct electronic commerce would hurt them and deny them the capability to exploit the stolen information.

Neglected Principles of War

Since the dawn of armed conflict, battles have traditionally been conducted in two dimensions. The beginning of the 20th Century saw war move into the third dimension through aircraft and submarines. Now as we are about to enter the 21st Century, warfare and the battlefield have expanded into yet another dimension, cyber-space. But no matter how foreign this new electro-magnetic spectrum may seem, the study of military history tells us that the introduction of new technologies and new battlefields do not change the basic principles of war. It only changes the way those principles are applied.

In the past, particularly in conventional war, adversaries were easier to identify and determining an enemy's presencewas a straightforward process. Information War, as discussed below, is more like fighting terrorists than conventional foes and presents similar difficulties in how to accurately identify and categorize adversaries. Even so, the Principles of War still apply.

Terrorism's effectiveness is based on the correct identification of a center of gravity and the efficient strike at it. Terrorists have a great advantage in dealing with national organizations in that they can accomplish limited objectives by striking just the right blow at the right time. And they can accomplish it with very limited resources. Information Warfare is similar in that it does not take many resources and with the correct target the result can be devastating.

Information Warriors are also analogous to terrorists in that they are susceptible to similar weaknesses.. Both require security and obscurity to operate most effectively. Nations that provide support can be a weakness to these organizations in that they can be pressured through more conventional means. Terrorist organizations tend to be as small as possible and not very robust. They can be made totally ineffective with a very small loss. An Information Warfare cell can be characterized in much the same way. To maintain security, Information Warrior organizations are as small as possible since the larger the organization the greater the chance of compromise. Lean organizations, once identified and located, can be destroyed or disabled by very small strikes.

In the following paragraphs we identify five of the twelve Principles of War that we believe are being neglected by most of the defenders in Information Warfare. They are all related to the singular concept of not being able to win a war by maintaining a defensive posture.

Offensive

Seize, retain, and exploit the initiative [2]

It takes a tremendous amount of resources to mount a strong defense everywhere at all times. The only way to avoid unacceptable costs while maintaining adequate defenses is to take the initiative in Information Warfare. On the offensive we, and not the enemy, dictate the conditions for battle. A determined adversary given enough time and resources will always be successful. A sound defense is critical, but it cannot hold out indefinitely. By targeting the enemy we can deny him both the time and resources necessary to defeat our defenses. This means that the response must be severe enough to stop the enemy attacks.

The key is to seize the initiative from our adversaries. When we only react to attacks, the enemy has the initiative. When we identify an attack before it occurs, take steps to nullify the attack or remove the enemy's means of conducting attacks we are following the principle of the Offensive.

This entails more than just sitting back with our new improved intrusion detection system and "putting our finger in the dike". Nor do we just clean up after its over. Instead we work to determine what he is going to do in advance. Our reaction is to not shut off their favorite attack, but to determine as much about the nature of the attacker as possible. We play defense until we have enough information to identify their center of gravity and then we go after it. If we have correctly identified the enemy's center of gravity we can decisively defeat him.

Maneuver

Place the enemy in a position of disadvantage through the flexible application of combat power [2].

Maneuver is the guiding principle in fighting an offensive war. It is the way we retain and exploit the initiative. Once we gain the initiative we keep it by making the enemy react to our actions until we can strike a decisive blow. We set traps, we block vulnerabilities, and we present the adversary with disinformation. When the opportunity presents itself, we strike the enemy's center-of-gravityand win.

We use maneuver both offensively and defensively. We maneuver to keep our adversary from defeating us in cyber-space while we identify his center of gravity. When ready we counter-attack to defeat the enemy. Maneuver in support of the defense involves the actions we take to minimize vulnerability and to retaliate against the enemy in order to keep him off balance. It exploits his potential weaknesses while protecting our own forces. It also serves to preserve our own freedom of action and reduces our own vulnerability. It continually creates new difficulties for the enemy by reducing the effectiveness of his actions and eventually leads to his defeat.

The use of maneuver in information warfare also requires agility of thought, plans, operations, and organizations just as it does in other more traditional levels of war. It requires designating and then shifting points of main effort while at the same time using the principles of surprise and economy of force.

While normally thought of in terms of physical movement of forces, maneuver in an age of information technology takes on new meaning and dimensions. As described by Leonhard [3], maneuver becomes a subset of the concept of dislocation, which has a desired end state of a disadvantaged enemy. In its purest form, dislocation is "the art of rendering the enemy's strength irrelevant p. 64" [3]. Technology, which is the weapon of choice for the enemy, becomes the counterforce that we maneuver or use. In effect its use denigrates the enemy's effort to a state of dysfunctionality.

Security

Never permit the enemy to acquire unexpected advantage. [2].

Warfare has always been about information. The difference now is that Information is the goal of militant actions. Armies have always tried to operate under a cloak of secrecy and where they have not stand examples of defeats. One of the best examples is the operation that spawned the computer age, the allied code breaking during World War II. Security is critical to properly defending information assets. The ease that attackers have in finding out about our infrastructure causes much of the problem. However, a cloak of secrecy is key to many counter-actions in Information Warfare. Disrupting information integrity of an adversary such that they loose their financial support is only effective as long as the target of the misinformation does not know that the operation occurred.

Most offensive actions will only be effective if the enemy does not know that he is under attack. In the current environment, our adversaries can operate with a well-founded sense of security. This allows them to put more resources into attacks against us and makes devastating attacks by small and under-funded adversaries possible.

Surprise

Strike the enemy at a time or place or in a manner for which he is unprepared [2]

Surprise and security generally go hand-in-hand. They each enhance the other and have a synergistic effect. We cannot allow ourselves to be surprised and we must also catch the enemy when he is least prepared. In information warfare most attacks can be deflected or at least mitigated if you know they are coming. Much of the success in attacks involves exploiting new vulnerabilities.

A military operation that the enemy does not expect has a much higher probability of success. War in cyberspace

certainly follows this principle. New types of attacks or attacks in new areas always meet with great success initially. Once counter-measures are developed and distributed the success rate falls dramatically.

Deception plays an important role in employing the principle of surprise. In a conventional sense, deception is usually combined with maneuver to put the enemy at a disadvantage. One of the best examples was the invasion of Europe by the allied forces in World War II. Because the German's believed that Patton was leading the main invasion in the South the Allies were able to establish a beachhead in Normandy. Information Warfare lends itself very well to deception operations. Encouraging attackers to expend energy and resources to attack the wrong systems could be useful in many situations as well as deceiving the enemy as to who is conducting counter attacks or the nature of counter attacks.

Economy of Force

Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary efforts. [2].

We cannot be strong in all places at all times. We must use our security resources wisely. We cannot hire enough security specialists to protect the entire National Information Infrastructure from attack. We cannot hire enough people to find every possible vulnerability before the enemy locates and exploits them. We would bankrupt the country before we plugged all the holes.

Currently, most of our IW adversaries operate without fear of retaliation. By striking back at attackers, the cost to them of their attack goes up. The possibility that we may retaliate against them means that they have to devote more resources to defensive measures. The larger and more resource intensive the organization must be to threaten our national security, the easier it is to identify and defend against and the fewer there will be.

For individual organizations that we attack we will not only reduce that specific attacker's ability, but effective counter strikes would be a strong deterrent to other potential adversaries. In a conversation with one of the authors in 1997, the chief of network security for a headquarters in the Pentagon said he detected about 80,000 attacks per month. The shear volume made it impossible to effectively defend his networks. If his section employed the offensive principles we espouse his job would have been more tractable. As word of aggressive and timely counter-attacks spreads throughout the cracker community the majority of these nuisance attacks could be eliminated allowing him to focus on identifying the serious threats and taking more effective counter measures.

Conclusion

So far we have fought information warfare defensively. We wait for an attack, recover, and take steps to prevent similar types of attacks. All the while the attacker is able to create new attack methodologies. Our resources are drained in this ever-increasing need to defend against known methods. It is imperative to take the offensive; not necessarily to become the aggressor in cyber-space, but when engaged to fight to win.

Once a strike is made we must employ maneuver and deception while gaining information about the perpetrator. Analysis of that information provides the necessary factors leading to the determination of the adversary's center of gravity. Then we make plans to seize the initiative from the adversary and attack his center of gravity.

The offensive action against this center of gravity must be aggressive, swift and clearly intended to destroy it. Surprise must be employed to prevent the enemy from engaging protective measures of their own. Economy of force needs to be used such that all our efforts are precisely focused and meet together at the critical place and time of attack.

Information Warfare that threatens our national security must be fought, like conventional wars, to win. The Principles of War have survived the test of time. As technology has changed, the application of the principles has changed but not the intent. We are currently fighting information wars by neglecting key principles of war. Those principles are offensive, maneuver, surprise, security and economy of force. The result will be our defeat and the weakening of our national security.

REFERENCES

1. Alberts, David S., *Defensive Information Warfare*; National Defense University, Directorate of Advanced Concepts, Technologies, and Information Strategies. 1996.
2. Field Manual 100-5, *Operations,* Headquarters, Department of the Army, Washington, DC, 14 June 1993.
3. Leonhard, Robert R., *The Principles of War for the Information Age*, Novarto, CA: Presidio Press, 1998.
4. Denning, Dorothy E. *Information Warfare and Security*, Reading, MA, Addison Wesley, 1999.
5. Joint Pub 3-13, Joint Doctrine for Information Operations, U. S. Department of Defense, 9 October 1998.
6. Sun Tzu, *The Art of War*, edited by James Clavell, Delta, 1983.

7. Goan, Terrance. "A Cop on the Beat: Collecting and Appraising Intrusion Evidence," *Communications of the ACM* 42(7) July 1999.
8. Durst, Robert, Terrence Champion, Brian Witten, Eric Miller, and Luigi Spagnuolo. "Testing and Evaluating Computer Intrusion Detection Systems," *Communications of the ACM* 42(7) July 1999.
9. Stillerman, Matthew, Carla Marceau, and Maureen Stillman. "Intrusion Detection for Distributed Applications," *Communications of the ACM* 42(7) July 1999.
10. Jajodia, Sushil, Catherine McCollum, and Paul Ammann. "Trusted Recovery," *Communications of the ACM* 42(7) July 1999.
11. Chin, Shiu-Kai. "High-Confidence Design for Security," *Communications of the ACM* 42(7) July 1999.
12. Douhet, Giulio. The Command of The Air, translated by Dino Ferrari and originally published in 1942, reprinted by the Office of Air Force History, Washington, D.C. 1983.
13. Cohen, Fred. *Managing Network Security Returning Fire*, On-Line. February 1999, accessed 29 July 1999. Available from **Error! Bookmark not defined.**. Internet.
14. Schartau, Winn. *Information Warfare*, Thunder's Mouth Press, New York, 1994.