

A Combined Offensive/Defensive Network Model

*Anthony Ruocco, Nathan Buchheit, and Daniel Ragsdale
Department of Electrical Engineering and Computer Science
Information Technology and Operations Center
United States Military Academy
West Point, New York 10996*

Abstract

Most literature on network modeling takes a functional perspective. That is, it models the network based on the needs the network must serve. As information assurance has risen as a functional need, the network models have added the need for a protective stance. In almost all instances, such a stance has been defined in terms of firewalls. As cyberspace becomes the next sphere of warfare, we must re-look networks in terms of the principles of war. No matter how robust the firewall, it is basically a defensive measure, and therefor doomed to failure in achieving victory. In preparing for information warfare, the underlying assumptions must be the intent for victory. This paper expresses some new insights on network modeling which emphasize the principles of *Offense, Maneuver, Security, Surprise, and Economy of Force*. Many of the concepts are intended to be thought provoking rather than advocating any particular action. We do not advocate any action that may be considered under today's laws and policies as illegal. Instead, by bringing out the restrictive nature of such policies we can reconsider options that prevent us from waging a "no-win" information war.

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 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 respect to the first element mentioned, in order to achieve victory in 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 goal. 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, rather 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

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.

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 highlights the futility of engaging in only a defensive war. Save the convergence of extreme circumstances taking a purely defensive posture tends to result in the attacker 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. 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 take advantage of the best offensive technology. They were able to prepare their battle plans without interference, and in fact much of Europe discounted any indication that Germany was even engaging in offensive planning. The end result was 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. The U.S. never forced North Vietnam to defend itself. This gave the North Vietnamese time to strike a fatal blow to the U.S. center of gravity- public support. Although wars are complex and these examples are simplified, history has shown us the folly of trying to fight a defensive war time and again.

Making a leap from physical combat to cyber combat may seem extreme. 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. It is almost always based on defending against the "last known type" of attack. In effect, it is the Maginot Line mentality applied to electronic bits. 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. There is frequently some loss associated with this vulnerability [time based security reference]. A determined attacker will eventually discover a new vulnerability after a new patch is installed. Fred Cohen has made the case that sitting back and waiting for attackers is a strategy doomed to failure [13].

Fighting an Information War offensively does not necessarily mean that we must assume the role of the aggressor. It 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.

The Combination Model

The network model we envision consists of several modules. There is the network itself that is a physical entity with operational characteristics. There is a virtual network with the same operational characteristics as the physical network. There is an identification module that probes the assailant module. The identification module serves to identify the type of assault as well as helping to identify the type of assailant. A module within the network makes use of the results of the probe to determine the assailants information target. Another module determines the value of the target information and a module exists which can conduct countermeasures. Finally, there is a module which is a history of all actions, and which serves as a knowledge base for future reference.

These modules interact in fairly specific ways as seen in Figure 1. Within the figure the squares represent physical entities and the ovals represent predominantly software entities. When an attack is suspected (a) it is immediately shunted to a virtual network (b). This virtual network can be a physical network, or a simulated network. But whatever implementation is taken, it must behave the same as the actual network. Once the shunt takes place, only the virtual network responds to the attacker (c). At the same time, the history/knowledge base is contacted. There may be enough information to make a decision on who the attacker is and their goal. It is critical to identify the attacker goal if an appropriate countermeasure is to be taken. If sufficient information is lacking then the systems contacts the ID Attacker module (d) that begins probing of the attacker (e). Concurrently (d), the knowledge base contacts a module that begins a process of identifying the most likely information target. As determinations are made on the information target, another process (f) begins determining the value of the information being sought after. It uses this information to propose an appropriate (i.e. measured) response. At the

same time, results of probes are placed into the knowledge base (h). These results are also used to determine the probable information target. Hence, though not shown in the diagram, there is actually a cycle of information passing between several modules as more information about the attacker become known. Based on the amount of information available, one countermeasure may be to pump false information into the virtual network (j). By providing false information of various details, it may be possible to gather information by probing the attacker response to the “new” information available. This can provide greater detail for determining the target of the attacker, or for identifying the type of attacker, and subsequently refining the selection of the countermeasure to be employed.

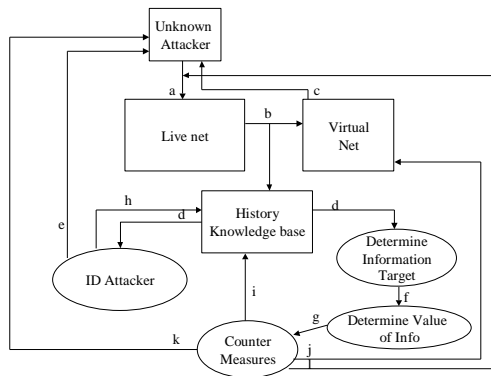


Figure 1: Modules and Interactions

The model is supported through current, and ongoing, research efforts. Much of the information concerns detecting intrusions and then amplifying the strength of the system firewall and other strictly defensive measures, e.g. better access control or password management approaches [Army R&D]. The Information Technology and Operations Center of Excellence is currently undertaking research in determining the return-on-investment of various network countermeasures against the value of the information being protected. It is also conducting research in the areas of using rule-based systems to identify types of incursions and the system vulnerability against those types of incursions. These approaches, valid in today’s environment and permissible under current laws, serves to force the network into a defensive, and hence unwinnable. Instead, we should focus on how the model better supports previously ignored principles of war.

Supporting the 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 deeply 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 following paragraphs we identify some of the twelve Principles of War that we believe have been neglected by most of the defenders in Information Warfare. We show how our model supports these principles, moving us from a purely defensive posture to one that can support the offensive.

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.

This entails more than sitting back with our new improved intrusion detection system and "putting our finger in the dike". By taking advantage of the ability to probe the enemy, develop knowledge bases about previous attempts and intrusions, and likely targets, we are able to seize the initiative through an attack. Within the model, this is accomplished through the modules which identify the attacker, develop and utilize knowledge base and employ proper countermeasures – branches e,h,d,k, l. Notice that branch l is simply a denial of access to the network, in other words, the current basic approach to intrusion detection.

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 misinformation. When the opportunity presents itself, we strike the enemy's center-of-gravity and win.

We use maneuver both offensively and defensively. We maneuver to keep our adversary from defeating us in cyberspace 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.

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]. The model utilizes maneuver by feeding false information (branch j) into the virtual network thus directing where the enemy may proceed or by noting enemy reaction to misinformation.

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 lose 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. By carefully developing countermeasures, and by using, possibly remote, probing techniques the enemy may be lulled into a false sense of security, only to discover too late that they have been detected.

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. 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. As seen in the model, one of our countermeasures may simply be in keeping the enemy focused on attacking the virtual network or the false information we have planted in the virtual network.

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 sheer 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. Coupled with this is the understanding that not all information is of equal value. We should not expend great deals of resources protecting and the return-on-investment portion of the model (d, f, g) help determine the resources to employ.

Conclusion

So far we have fought information warfare defensively and network models focus on the firewall. We wait for an attack, recover, and take steps to prevent similar types of attacks. Network models support the continuous addition of patches, yet never account for resources which are drained in this ever-increasing need to defend against known methods. It is imperative that we stop looking at the network as a dormant entity but instead consider it a major battle system with capabilities of its own. As such, the models we use to develop networks should be oriented on the principles of war.

Our model takes a much more dynamic view of the network. Initially the network remains in a defensive state. It relies on firewall protections as well as access management policies. In other words, a very traditional network view. Then, once attacked, the network becomes proactive. It can determine the attacker, determine the information under attack, and determine the best means of protecting that information. If necessary, the network becomes capable of taking offensive operations from a solid defensive position.

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*, Novato, 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 <http://all.net.journal/netsec/9902.htm>. Internet.
14. Schwartz, Winn. *Information Warfare*, Thunder's Mouth Press, New York, 1994.
15. Schwartz, Winn. *Time Based Security*, Interpact Press, Seminole Florida, 1999.
16. Buchheit, Nathan, Anthony Ruocco, and Donald Welch, "Strike Back: Offensive Actions in Information Warfare," 22nd National Information Security Conference, Arlington VA, Oct 99.