Proceedings of the 2001 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY, 5-6 June, 2001

Principles of Cyber-warfare

Raymond C. Parks and David P. Duggan

Abstract-- **This paper proposes some principles of cyber-warfare. The principles of warfare are well documented, but are not always applicable to cyber-warfare. Differences between cyberspace and the real world suggest some additional principles. This is not intended to be a comprehensive listing of such principles but suggestions leading toward discussion and dialogue.**

The current candidate list of principles of cyber-warfare includes the following.

Cyber-warfare must have kinetic world effects.

One can take active steps to hide in the cyber world, but everything one does is visible; the question is whether someone is looking.

There are no immutable laws of behavior in the cyber world except those that require a physical world action to change.

Some entity within the cyber world has the authority, access, or ability to perform any action an attacker desires to perform. The attacker's goal is to assume the identity of that entity in some fashion.

The tools of cyber-warfare are uniquely dual-use.

Both the defender and the attacker control a very small part of the cyberspace they use. Whoever can control a part of cyberspace that the opponent uses can control the opponent.

Cyberspace is not consistent or reliable.

Physical distance from the target is almost irrelevant.

***Index Terms*--.**

I. Introduction

Cyber-warfare requires different principles of warfare from kinetic warfare. Classic, kinetic warfare principles have been derived from thousands of years of experience as documented by Sun Tzu, Clausewitz, Jomini, Liddel-Hart, and others. Some of the kinetic warfare principles apply to cyber-warfare while some principles of kinetic warfare have no meaning in cyber-warfare. Some principles of kinetic warfare may actually be antagonistic to cyber-warfare.

The principles of cyber-warfare discussed in this paper are derived from the bottom up. As part of Sandia National Labs' Information Design Assurance Red Team (IDART), we have hands-on experience at conducting limited cyber-warfare. While conducting active adversarial analysis of information systems, the authors have "discovered" eight principles of cyber-warfare. This is not an exhaustive list, nor is it intended as the final definitive list. Instead, these principles should be taken as a starting point for discussion within the cyber-warfare community.

For the purposes of presenting the principles of cyber-warfare, we must provide our definitions of terms. Cyber-warfare is the sub-set of information warfare that involves actions taken within the cyber world. The cyber world is any virtual reality contained within a collection of computers and networks. There are many cyber worlds, but the one most relevant to cyber-warfare is the Internet and related networks that share media with the Internet. The closest military definition to our term, cyber-warfare, is a combination of computer network attack and computer network defense, and, possibly special information operations. [1].

We define kinetic warfare as warfare practiced in the "real world". All the tanks and ships and planes and soldiers of current militaries are the protagonists of kinetic warfare.

Kinetic warfare has a history as long as mankind's that includes many attempts to derive principles for practitioners. Military men and others have attempted to pass on the wisdom and insight they have gained, usually through hard lessons. Tsun Tzu's The Art of Strategy [2] is frequently cited in publications about information operations. It's primary relevance to cyber-warfare involves our first principle that cyber-warfare must have a real world effect. Tsun Tzu recommends manipulating the decision-making of the adversary. Clausewitz' Von Kriege [3] seems to have lost popularity with writers about Information Operations, but we believe it still has relevance, particularly the thoughts on will, the fog of war, and the friction of war. Cyber-warfare as a part of information operations can affect the will of the enemy to fight. Strategic cyber-warfare attacks proposed for the theoretical exercises and workshops have been aimed at increasing the fog and friction of war. Liddel-Hart's Strategy [4] is applicable to cyber-warfare through the principle of the indirect approach. In our experience, cyber defenses are best handled, from an attackers point-of-view, by avoiding them altogether. In most exercises that have had defenses we, as attackers, have either bypassed the defense or ignored it.

We have no intention of traversing an exhaustive list of kinetic warfare principles for this paper. We considered the principles primarily to isolate those principles of cyber-warfare that are different from kinetic warfare. A useful consolidation

Manuscript received March 26, 2001 This work was supported in part by the Defense Advanced Research Program Agency under Agreement #01K410.

Raymond C. Parks is a Senior Member of the Technical Staff with Sandia National Laboratories, Albuquerque, NM 87185-0455 USA (telephone: 505-844-4024, e-mail: rcparks@sandia.gov).

David P. Duggan is a Senior Member of the Technical Staff with Sandia National Laboratories, Albuquerque, NM 87185-0449 USA (telephone: 505-845-8100, e-mail: dduggan@sandia.gov).

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE

of the writings on kinetic warfare can be found in Appendix B of JP-1 [5].

The kinetic principles we have chosen to examine are those of mass, objective, offensive, surprise, economy of force, maneuver, unity of command, security, and simplicity. The kinetic principle of *mass* is largely irrelevant to cyber-warfare except when engaging in Denial of Service (DOS) attacks that simulate kinetic warfare actions. The kinetic principle of *objective* is certainly applicable to cyber-warfare. Our adversary models include the principle of objective as part of all types other than unsophisticated crackers [6],[7]. The kinetic principle of *offensive* is not particularly important in cyber-warfare. Cyber-warfare is different from conventional warfare in that stealth and surprise are supremely important. At the Cyber Strategy Workshop in October of 1999, analogies were made between cyber-warfare and submarine warfare and cyber-warfare and special operations. Both of these analogies are suitable in our opinion. We have been told that our cyber-terrorist model closely matches the operational profile of assassins. In none of these cases is the offensive as important as in conventional warfare. The kinetic principle of *surprise* applies to cyber-warfare. Cyber-warfare is inherently an application of the kinetic principle of *economy of force*. Since cyber-warfare is the epitome of asymmetric warfare, economy of force is inherent. The kinetic principle of *maneuver* is applicable to cyber-warfare. The attacker isn't moving their forces, just the point of attack. The kinetic principle of *unity of command* is applicable to cyber-warfare in certain circumstances; however, there are certain cyber-warfare attacks that use unwitting masses of bystanders who are not within the command of the protagonist. The kinetic principle of *security* applies to cyber-warfare. The kinetic principle of *simplicity* applies to cyber-warfare – we call it going after low-hanging fruit!

Our research for this paper revealed that the umbrella term, information operations, which includes cyber-warfare carries a lot of baggage with it. We do not intend to comment on the controversies over whether information operations constitutes a Revolution in Military Affairs (RMA), which government organization should control information operations, or what laws have to be changed for cyber-warfare to be legal. We are basing most of this paper on our observations of how things really work, on-line and active. We have experience with 51 red-teaming activities ranging from planning attacks through white-boarding exercise to actual hands on engagements.

II. Candidate Principles of Cyber-warfare

A. *Cyber-warfare must have kinetic world effects*

Cyber-warfare is meaningless unless it affects someone or something in the non-cyber world. One can attack entities in the cyber world as much as one wants, but unless something happens in the physical world as a result, one might as well be playing corewars. Cyber-warfare can affect an object in the physical world such as the opening of a dam spill-gate or shutdown of an electrical sub-station. Cyber-warfare in its most subtle form can affect the minds of decision-makers in the physical world. The former is analogous to kinetic warfare. The latter is more purely a form of information warfare, in which one's opponent is presented with information that leads to wrong decisions.

Examples of affecting physical world entities abound – we have proposed attacks that would manipulate an electrical power-grid into failure and that would open the floodgates of dams. We have proposed attacks that would cause railroad accidents. The list of possible physical entities that can be affected looks very much like the list of Y2K problems.

Examples of affecting decision-makers include both tactical and strategic decision-makers. Tactical decision-makers can be misled about the location and size of enemy and friendly forces. At an operational level, the time of arrival and amount of supplies and reinforcements can be manipulated to cause bad decisions such as attacking with insufficient ammunition or withholding attack through fear of lack of supplies. Strategic decision-makers may be fooled by attributing actions to other countries or groups than the actual attacker. We co-developed the scenario for a DARPA workshop that centered on an adversary attempting to foment war between the US and another country via cyber-warfare. The participants playing the role of the National Command Authority (NCA) could not determine the real adversary.

B. *One can take active steps to hide in the cyber world, but everything one does is visible; the question is whether someone is looking..*

The cyber world is an artificial one, created by human beings using hardware and software. Any actions that a combatant takes in that world require the movement or manipulation of data. The very fact that one attempts to conduct cyber-warfare means that some bit in some data stream is changed to reflect one's presence and actions. This is good news to defenders. However, this is only useful to the defender if they are looking; and there's the rub. Our experience can be summed up in the sound-byte "Sensors don't".

The analogy to hiding in cyber-warfare is the physical world use of camouflage. The physical world combatant can take active steps to modify their sensor footprint – witness stealth technology. In the cyber world, the combatant cannot take active steps equivalent to absorbing radar energy or cooling infrared signatures. Instead, the cyber-warfare protagonist must try to hide the evidence within the existing data streams. Sensors looking for cyber attacks have to distinguish between bits that are an artifact of the attacker and the overwhelming majority that are normal activity. This is made more complicated by using normal activity to conduct an attack. Intrusion detection systems cannot distinguish between a normal database user and an adversary manipulating the database as that user.

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE

C. There are no immutable laws of behavior in the cyber world except those that require a physical world action to change.

In the physical world, one can expect that a bullet will act in a certain way when fired. The bullet's path can be predicted with ballistics. Every time that one fires the bullet, it will act the same, within a variance due to minor physical causes. In the cyber world, nothing can be taken for granted in this way. The cyber world, as an artificial construct of humans, is imperfect. It can and does change in ways that seem chaotic. Software fails, hardware fails, programs run faster than expected, and a thousand other variations cause the unpredictability of the cyber world.

In cyber-warfare, this principle translates to attacks that don't always behave the same way, environments that change, and fluctuations in performance. The only aspects of the cyber world that do not change are those things that require a physical world change. For example, the performance of software cannot exceed the capacity of a computer's processing power unless a physical world person changes to a faster processor. The bandwidth of communications is limited by the telecommunications infrastructure and can only be changed by replacing one physical layer with another.

An example of real-world experience that supports this occurs during sniffing of packets. We frequently see one set of connections and packet streams during discovery only to find a different set when we attempt our attack.

D. Some entity within the cyber world has the authority, access, or ability to perform any action an attacker desires to perform. The attacker's goal is to assume the identity of that entity, in some fashion.

Since the cyber world is a purely artificial construct, it is built and controlled by humans and their tools. There is no part of the cyber world that is not controlled by someone or his agent. Sometimes the entity with the authority, access or ability is the avatar of a human being. Sometimes the human has passed the control to a software element. But there is always something or someone who can do what the cyber-combatant wishes to do. Most of the steps in any attack in cyber-warfare are simply intended to assume the identity of the entity that can perform the desired action.

The classic example of this is the UNIX root exploit. When one performs a root exploit, one is attempting to assume the identity (and therefore authority, access, or ability) of the root superuser of a UNIX system. In our exercises, we have used root exploits as steps in attacks that involved changing the configuration or software of the target systems.

However, the root exploit is not the only example, nor even the most common. During the course of many exercises, we have discovered and stolen the identities of ordinary users, database administrators, system programs (such as UNIX daemons and Windows services), and developers. In every case, we first found out who or what could perform the action and then worked to assume that identity.

E. The tools of cyber-warfare are uniquely dual-use.

The tools of kinetic warfare are primarily used for a single purpose. Weapons are used to attack, armor is used to defend, and sensors are used to detect the enemy. During actual warfare, one does not test one's defenses by shooting your own troops. The commander of an ambushing unit uses his night-vision gear to look for the enemy. He can, but rarely does, walk out to where he expects the enemy to be and look at his own troops with that night-vision gear.

In cyber-warfare, tools are used by both the attacker and the defender. The attacker uses vulnerability scanners to look for exploit opportunities as part of an attack. The defender uses the same vulnerability scanners to look for weaknesses in their own systems. Packet capture devices originated because network administrators had to see the actual packet traffic to diagnose network problems. Attackers use them for discovery. Specific exploits are collected by defenders to test their own systems, since those systems can regain vulnerabilities from poor vendor upgrades.

F. Both the defender and the attacker control a very small part of the cyberspace they use. Whoever can control a part of cyberspace that the opponent uses can control the opponent.

The attacker and defender in cyber-warfare can control only that hardware and the software that they own. Frequently, this limit is their actual physical perimeter. Rarely does a cyber group control anything beyond their interface with the communications infrastructure. It was hypothesized that DoD only controls 10% of the communications infrastructure used for DoD traffic. This means that neither the attacker nor defender control 90% of the infrastructure they use in the course of their activities.

Even if neither party in cyber-warfare control the infrastructure they use, they are still vulnerable to attacks on that infrastructure. If one or the other can gain control of part of that infrastructure, the advantage goes to that controller.

A frequent attack that we use is to gain control of the Domain Name Service (DNS) upon which a target relies. We have done this by directly attacking the DNS server or by spoofing replies from the server. Once we have control of that DNS, the target is vulnerable to many types of spoofing attacks. For example, we used this type of attack to bypass an implementation of Internet Protocol Security (IPSEC) during a DARPA exercise in June of 2000.

G. Cyberspace is not consistent or reliable.

Yet another artifact of the artificial nature of cyberspace is that it is not consistent or reliable. This is related to the principle about immutable laws. Neither hardware nor software will always work as expected in cyberspace. This is true more of software, but we have seen inconsistency in hardware, usually due to heat or power loads.

One effect of this principle is that one can never be certain that a step within an attack will work. In one exercise, we carefully collected local root exploits to use after user access

to a known version of Solaris had been achieved. We were frustrated, however, to find that none of the exploits worked, despite being aimed at the correct version of Solaris. Instead, one of the administrators of the target network informed us that a variant of an exploit that was supposedly fixed two versions earlier worked quite well. In a recent exercise, we conducted scans of target systems with multiple tools. We then spent time trying to understand why the results of the scans were so different!

An opposite effect of the lack of consistency or reliability is that attacks one does not expect to succeed frequently do so. We believed that the defenders had successfully hidden open password traffic within a VPN in another exercise. Much to our surprise, they had left one service outside of the VPN that provided us with the necessary password to login as the database administrator. That particular exercise taught us that high payoff exploits should be tried even if we don't expect them to succeed.

H. Physical limitations of distance and space do not apply to the cyber world.

In cyber world, physical distance is not an obstacle to conducting attacks. A cyber attack can be executed with equal effectiveness from the other side of the earth as from the next room. In kinetic warfare attacks are carried out by physical objects that must traverse a distance. These types of attacks are limited to those that possess the technology to make that object traverse that distance.

The acquisition of appropriate mass in the kinetic world has physical limitations. The creation of mass in the cyber world does not seem to have this limitation.

III. CONCLUSION

Cyber-warfare is different from conventional, kinetic warfare. Both it and its parent, information warfare, depend upon the frailties of human beings for many characteristics. One of the fundamental differences between cyber-warfare and kinetic warfare is the nature of their environments. Kinetic warfare takes place in the physical world, governed by physical laws that we know and understand. Cyber-warfare takes place in an artificial, man-made world that is chaotic with imperfections. Cyber-warfare can use some of the principles of kinetic warfare, but there are other principles that have little or no meaning in cyberspace. For these reasons, the principles of cyber-warfare are, ultimately, different from those of kinetic warfare.

REFERENCES

[1] Department of Defense Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998.

[2] Tsun Tzu, *The Art of Strategy*, edited and translated by R. L Wing, Doubleday, New York, 1988.

[3] Carl Von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret, Alfred A. Knopf, New York.

[4] B. H. Liddel-Hart, *Strategy*, Second Revised Edition, Frederick A. Praeger, New York.

[5] Department of Defense Joint Publication 1, Joint Warfare of the Armed Forces of the United States, 14 November 2000.

[6] Gregg Schudel, Bradley Wood, Raymond Parks, "Modeling Behavior of the Cyber-Terrorist", National Security Forum on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, 6 December 1999.

[7] Ruth Duggan, Insider Adversary Model Briefing, DARPA IASET Insider Workshop, August 2000.

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE