# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| 09 February 2004 | FINAL | |

**4. TITLE AND SUBTITLE**
CYBERWARFARE

Ulysses Bow or Achilles Heel for the Combatant Commander?

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
LCDR Sonya Cox, United States Navy

Paper Advisor (if Any): Doug Hime

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Distribution Statement A: Approved for public release; Distribution is unlimited.

**13. SUPPLEMENTARY NOTES** A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

**14. ABSTRACT**

**Just as the advent of precision-guided weapons has significantly reduced and limited collateral damage in modern technological warfare, so the emergence of cyber technology may produce a shift in the very way in which war is conceived in the twenty-first century, reducing the amount of collateral damage and the number of combatant casualties to the point it may be possible to subdue the enemy without bloodshed. The first line of attack In warfare has always been the adversary's ability to wage war through the destruction of his military and industrial infrastructure. In the rapidly evolving Age of cyber war, this might be accomplished with a minimum o physical destruction and human casualties. Today's Combatant Commanders can and should take advantage of the new capabilities that cyber warfare offers, while maintaining a secure defensive posture in order to protect them where they are most vulnerable.**

Cyber-warfare, Information Operations, Asymmetric Warfare, Computer Network Defense and Attack

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | Chairman, JMO Dept |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | 19 | **19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556 |

**Standard Form 298 (Rev. 8-98)**

NAVAL WAR COLLEGE

Newport, R.I.

# CYBERWARFARE:
# Ulysses Bow or Achilles Heel for the Combatant Commander?

by

**Sonya Cox**
Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Strategy and Policy Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

09 February 2004

**To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.**

**Sun Tzu, The Art of War**

## INTRODUCTION

Just as the advent of precision-guided weapons has significantly reduced casualties and limited collateral damage in modern warfare, so the emergence of cyber technology may produce a shift in the very way in which war is conceived in the twenty-first century, reducing the amount of collateral damage and the number of combatant casualties to the point where Sun Tzu's ideal may indeed be an achievable goal. The first line of attack in warfare has always been the destruction of the adversary's military and industrial infrastructure. In the rapidly evolving age of cyber war, this might be accomplished with a minimum of physical destruction and human casualties. However, we must not allow ourselves to be deluded by the sense that this is a "sanitized" form of war, because the bottom-line impact may be no less catastrophic in its effect on the targeted society. Cyber warfare is a significant threat to our National Security. "Eight nations have developed cyberwarfare capabilities comparable to America's. More than 100 countries are trying to develop them. Twenty-three nations have cybertargeted U.S. systems, according to knowledgeable intelligence sources." [1] It is therefore vital that Combatant Commanders be ready to respond to such threats.

Today's Combatant Commanders can and should take advantage of the new capabilities that cyber warfare offers in order to achieve synergy while maintaining a secure defensive posture in order to protect them where they are most vulnerable. Joint

[1] CSIS Global Organized Crime Project, Cybercrime—Cyberterrorism—Cyberwarfare—Averting an Electronic Waterloo (Washington, D.C.: Center for Strategic and International Studies, 1998), xvi.

doctrine for information operations clearly states that the Combatant Commanders are responsible for incorporating defensive and offensive information operations into deliberate and crisis action plans to accomplish assigned missions.[2] That is easier said than done. This paper will examine some of the reasons why.

## WHAT IS CYBERWARFARE?

*Cyber* is a relatively new term that has entered the military vocabulary. According to Lionel D. Alford, cyber refers to "mechanical or electronic systems to replace human control."[3] In today's security environment, cyber war has become a form of information warfare, which is defined as "the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."[4] The current military mindset (though changing) is still focused more on traditional forms of warfare, thus making the cyber threat a real issue for the United States with which to deal. Critical vulnerabilities and centers of gravity are terms easier to comprehend when cyber issues do not have to be taken into account, because such warfare is newer and there are fewer written guidelines or practical experiences to which Combatant Commanders can relate. Potential adversaries have recognized, or soon will, that our

[2] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, D.C.: U.S. Government Printing Office, 9 October 1998): I-5.

[3] Lionel D. Alford, "Cyber-Warfare: A New Doctrine and Taxonomy." CrossTalk 14, no.4 (April 2001): 27; available from http://www.stsc.hill.af.mil/crosstalk/2001/04/alford.html; Internet; accessed 22 December 2003.

[4] Ivan Goldberg, Institute for Advanced Study of Information Warfare (IASIW) "Glossary of Information Warfare terms." available from http://www.psycom.net/iwar.2.html; Internet; accessed 27 October 2003.

lack of preparedness against potential cyber attacks will be a critical vulnerability that they may be able to exploit against the United States, especially since they cannot hope to defeat us in a conventional manner. "Security is no longer defined by armed forces standing between the aggressor and the homeland. The weapons of information warfare can outflank and circumvent military establishments and compromise the common underpinnings of both U.S. military and civilian infrastructure, which is now one and the same."[5]

## THREATS AND VULNERABILITIES

The new threats that are emerging, including those of cyber war, require new and different approaches to the dangers of this new national security environment. "While it is hard for some to believe, we are arguably in a more dangerous world with less means to defend our vital interests, with institutions that are less well structured and practiced to carry out needed operations. This is because the emerging threats are different and are continuing to evolve, as well as because our legacy force structure and concepts of operation are not well suited for the tasks at hand, nor are they agile enough to keep abreast of the continuing changes."[6] Though the military is continuing to strive towards better defensive capabilities, it needs to make sure it leverages the civilian resources and interagency assistance and cooperation, as well, in order to get the most from a combined effort of technologies and brainpower.

---

[5] CSIS Global Organized Crime Project, xiii.

[6] David S. Alberts, and Richard E. Hayes, Power to the Edge: Command, Control in the Information Age. With a Foreword by John Stenbit (Washington, D.C.: Command Control Research Program, DoD: June 2003): 2.

The United States is the most technologically capable country in the world, and therefore the most vulnerable due to its reliance on the information infrastructure it has adapted. "The Defense Department acknowledges between 60 and 80 attacks a day, although there have been reports of far more than that."[7] Cyber threats range from nation-state actors to the every day hacker, each with his own motives and destructive capability. Protecting our vulnerable infrastructure constitutes one of the biggest security challenges of our age. As the CSIS Global Organized Crime Project has pointed out, ". . . the United States keeps testing its own vulnerabilities. They are enormous. There is still no technology for pinpointing the source of a cyberattack."[8]

Examples of vulnerabilities which underscore America's reliance on information technology include an exercise conducted by DoD referred to as "Eligible Receiver." During this 1997 exercise, "A 'red team' of hackers from the National Security Agency (NSA) was organized to infiltrate the Pentagon systems. . . . Although many details about Eligible Receiver are still classified, it is known that the red team was able to infiltrate and take control of the Pacific command center computers, as well as power grids and 911 systems in nine major U.S. cities."[9] Although "Eligible Receiver" took place within the United States, the threat of cyber terrorism is global, therefore making this one of the Combatant Commanders' major responsibilities in today's environment.

---

[7] John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," CNN Interactive, 6 April 1999; available from http://edition.cnn.com/TECH/specials/hackers/cyberterror/; Internet; accessed 28 November 2003.

[8] CSIS Global Organized Crime Project, xvi.

[9] "Eligible Receiver," Cyber war Frontline. 24 April 2003; available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/; Internet; accessed 2 January 2004.

As another example of a vulnerability, Moonlight Maze was an actual incident that accidentally uncovered "a pattern of probing of computer systems at the Pentagon, NASA, Energy Department, private universities, and research labs that had begun in March 1998 and had been going on for nearly two years. . . [during which time] invaders were systematically marauding through tens of thousands of files—including maps of military installations, troop configurations and military hardware designs."[10] An incident of this magnitude and duration could have posed a serious threat to our national security if the "anonymous" attacker indeed had ulterior motives and turned the "probing" incident into actual disruption or destruction.

These are just a few examples of network attack vulnerabilities that exist. One must keep in mind that these are attacks that were "discovered." There is no sound approach to determine the extent of attacks that have actually occurred and possibly caused harm to our national security in ways that we may never realize.

Given the absence of a conventional front in modern cyber warfare and the rapidly evolving nature of the technology, the Combatant Commander is going to require new means, available resources and clear guidelines to fight, win and defend against asymmetric threats initiated from cyberspace. Our National Military Strategy dictates that we must include asymmetric threats in our preparations for the wars of tomorrow.[11] However, the threat of cyber warfare is an unprecedented form of asymmetric warfare for which the traditional military structure and response protocol were not designed. Given

[10] "Moonlight Maze," Cyber war Frontline. 24 April 2003; available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/; Internet; accessed 27 December 2003.

[11] Chairman of the Joint Chiefs of Staff. National Military Strategy of the United States of America (Washington, D.C.: U.S. Government Printing Office, 1997): 26.

the military's traditional orientation toward conventional warfare, potential adversaries will take advantage of the seams that have evolved in our command and control structure in dealing with cyber attack issues. The availability of the expertise and the resources to launch such attacks will make it an increasingly attractive form of warfare to potential enemies, whether nation states, insurgents, or terrorists.

The Chairman of the Joint Chiefs of Staff has realized the importance that cyber warfare will play in the future of military operations and has specified this in Joint Vision 2020 (JV2020), which states, "We have superior conventional warfighting capabilities and effective nuclear deterrence today, but this favorable military balance is not static. In the face of such strong capabilities, the appeal of asymmetric approaches and the focus on the development of niche capabilities will increase."[12] Given these new realities in the contemporary global environment, the Combatant Commander is facing a new kind of challenge that will require clear cut and precise approaches to fulfill his/her responsibilities.

When Combatant Commanders are tasked to respond to a situation and are in the first stages of developing their command assessment, they are accustomed to developing the plan based on traditional styles of warfare, considering the major actions to be played out in a typical "battlefield" scenario. As noted by Dr. John Hamre in a speech at a NATO workshop in Vienna on 22 June 1998, "It used to be that our national and alliance critical infrastructures were defined by geography and physical equipment—that is no longer true. There are no borders in cyber space. Critical infrastructure now includes a

---

[12] Chairman of the Joint Chiefs of Staff, Joint Vision 2020: America's Military Preparing for Tomorrow (Washington, D.C.: U.S. Government Printing Office, 2000): 4.

vast dependence on information systems. All of our nations depend on these systems to run our communications, power grids, air traffic control systems, hospitals, banks—all of our key functions."[13] A well-coordinated cyber-attack would probably target several of these critical infrastructures PLUS launch an attack on the military's cyber infrastructure to suppress a response.

We must be aware of the threat posed against our Combatant Commands in such an example. Considerable attention has been given to homeland security and defending the United States generally from cyber attacks, but what about the Combatant Commanders and their AORs? How are they to deal with possible threats of cyber attacks in their respective theaters? Every day hackers are dealt with by the FBI, but what guidance and structure does a Combatant Commander have in order to deal with threats against his/her area of responsibility, both defensively and offensively?

## CURRENT COMMAND AND CONTROL STRUCTURE

The United States military indeed realizes the emerging threat of cyber warfare issues and has attempted to form organizations to deal with it. The need to be responsive to cyber issues has been recognized by all services, as illustrated by the formation of agencies like the Air Force Information Warfare Center (AFIWC), the Land Information Warfare Activity (LIWA), and the Fleet Information Warfare Center (FIWC).[14] In an attempt to craft a common strategy to deal with cyber issues, Navy Secretary Gordon

[13] John J. Hamre, "Counter-Proliferation Efforts Must Include Defense Against Cyber Attacks," Defenselink 13, no.44 (22 June 1998): available from http://www.defenselink.mil/speeches/1998/s19980622-depsecdef.html; Internet; accessed 12 December 2004.

[14] Joint Command Control and Information Warfare Staff at the Joint Forces Staff College, Information Operations: The Hard Reality of Soft Power (Norfolk, VA.: Joint Forces Staff College, 2000), 15.

England authorized the creation of the Naval Network Warfare Command (NETWARCOM) with responsibility for all Navy information technology networks, information operations and space requirements.[15]

Such attempts at placing cyber issues to the forefront of military planning, examination and acquisition are to be applauded; however, the current military organization and command and control structure is lagging in its attempt to properly form itself into a seamlessly cohesive machine in order to deal with cyber warfare issues. Due to the very nature of the services, with so many agencies looking in different directions for cyber warfare guidance, it is extremely difficult for a Combatant Commander to find a single source of immediate, comprehensive guidance and policy when it comes to either dealing with an attack in his AOR or conducting offensive operations when the situation warrants. "The current state of planning for cyber-warfare has frequently been likened to the early years following the invention of the atomic bomb more than a half-century ago, when thinking about how to wage nuclear war lagged the ability to launch one." [16]

According to a recent Washington Post article, the Pentagon has recognized the need to establish an appropriate C2 structure by assigning responsibility for cyber warfare capabilities to STRATCOM and by appointing a special task force for the consolidation of offensive and defensive planning.[17] The latter decision is useful to the Combatant Commander because it provides "one" point of contact for dealing with cyber issues.

---

[15] Christopher J. Dorobek, "Navy Creates Network Command." Federal Computer Week, 27 March 2002; available from http://www.fcw.com/fcw/articles/2002/0325/web-navy-03-27-02.asp; Internet; accessed 9 January 2004.

[16] Bradley Graham. "Bush Orders Guidelines for Cyber-Warfare," Washington Post, 7 February 2003, A01.

[17] Ibid.

The Computer Network Attack (CNA) and Computer Network Defense (CND) missions are ones that will enable the Combatant Commanders to use cyber capabilities in order to support their objectives. The Joint Task Force-Computer Network Operations (JTF-CNO) is on the right path to delineating specific roles and missions required:

> For the CNA mission, the JTF-CNO is responsible for ensuring that CNA capabilities can be efficiently employed in support of U.S. National Security objectives. The JTF-CNO, along with the USSTRATCOM staff, services, other combatant commanders, and defense agencies, is working to develop and implement comprehensive policies, structures, roles and missions for computer network operations. The initial U.S. Strategic Command concept of operations calls for the supported commander, assisted by the JTF-CNO, to integrate service-provided forces into military plans and operations. USSTRATCOM will coordinate the use of all DOD CNA assets for the supported commander.[18]

These structure changes have indeed consolidated some important forms of dealing with cyber attacks into one area of responsibility in an attempt to better facilitate communication, guidance and direction from STRATCOM to the Combatant Commanders when dealing with cyber warfare issues and the need to prepare for them both offensively and defensively. But according to the CSIS Global Organized Crime Project, "The major-regional-conflict standard on which the U.S. military currently bases its planning is increasingly irrelevant as information systems become the more likely target of attack"[19] The current military policy for dealing with conflicts may be suitable for conventional warfare, but it could leave our forces unprepared to deal with major-regional-conflicts that are initiated through cyberspace. Cyber attacks can be global and

[18] United States Strategic Command, "Joint Task Force – Computer Network Operations." Fact Sheet, February 2003; available from http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm; Internet; accessed 29 November 2003.
[19] CSIS Global Organized Crime Project, xxi.

travel the full range of operations, encompassing ALL Combatant Commander areas of responsibilities in one shot.

As a typical example of how CNO can be integrated at the level of the Combatant Commander, United States Pacific Command (USPACOM) has a CND and Information Assurance Division within the J6 directorate; however, nothing related to CNA or knowledge of how other Combatant Commanders do business in their area is included. Based on interview responses from Major Calvert L. Bowen, Chief, Theater Information Assurance Support Branch for USPACOM, it is interesting to note that USPACOM does not have an established standard operating procedure for dealing with CNO attacks in theater.[20] Instead, each subordinate command is responsible for defending its own networks in accordance with its respective service requirements. Therefore, the procedures may not be the same.

Each command also has its own law enforcement office, which supports its operations. Moreover, throughout DoD, the host organization or "owner" of each military installation has the lead for initial investigations. Different standard operating procedures, law enforcement organizations and sets of service agency reporting criteria allow room for confusion due to the lack of streamlining. PACOM is aware of these issues and is continuously trying to improve the process, but due to the complex reporting chain and the existence of different communications systems among services and agencies, this is a huge challenge.

Because of a lack of interoperability among components of the current communication infrastructure across DoD, individual services in some cases still require

[20] Calvert L. Bowen, interview by author, email, United States Pacific Command, HI. 6 January 2004.

separate rules and service oriented organizations when dealing with cyber attack issues. Current command and control structure dealing with cyber attack issues is not yet standardized to best assist the Combatant Commander.

## CURRENT POLICY AND DOCTRINE

**Defensive Approach:** Within the Department of Defense, computer attacks are seen more as "crimes" rather than potential acts of war. Perhaps this perception exists due to the fact that potential enemies have not yet caused serious damage to our national security via cyber attacks. As Major Bowen points out, "if an intruder is found on a military base, then the local command can use standard law enforcement procedures to detain."[21] Bowen goes on to say that if a Combatant Commander is lucky enough to physically apprehend a cyber attacker in his AOR, there are numerous things to consider, like citizenship, confirmed identity, and various other issues. Also, since most network services in a Combatant Commander's AOR are provided by the individual services, those local commands should be the ones designated to take action. Since these issues are so new, and the likelihood of catching a cyber attacker is slim, procedures and guidelines for these issues are not clear. Again, as observed in the statements from Major Bowen, the current mindset of the military immediately approaches cyber attacks as "crimes" rather than potential attacks on our national security. The discovery of a "dirty" bomb or a nuclear device in the Pacific AOR would surely generate more than a local response or a follow-on incident report; given the magnitude of the potential threat to national security, the discovery of a cyber attack in the AOR should trigger a comparable

[21] Ibid.

kind of response up the chain of command. Procedures and guidelines must be made available to facilitate such a response. Considering the ramifications that could result from a cyber attack, it would seem reasonable to produce a separate document pertaining only to rules governing cyber warfare. "Unfortunately current Department of Defense (DoD) doctrines and instructions do not adequately cover the scope of cyber warfare [5]. Several handle information warfare as a discrete part of a military system. These include Joint Publication 3-13 Joint Doctrine for Information Operations (JP 3-13), Joint Publication 3-13.1 Joint Doctrine for Command and Control Warfare (JP3-13.1). . . ." [22] But cyber warfare in these publications continues to be treated as just another form of information warfare.

**Offensive Approach:** With the emergence of potential offensive capabilities for cyber warfare, the current administration is taking a proactive approach to establishing appropriate policy. As Bradley Graham noted in the February 7, 2003 edition of the Washington Post, President Bush has issued a secret directive (National Security Presidential Directive 16) "ordering the government to develop, for the first time, national-level guidance for determining when and how the United States would launch cyber-attacks against enemy computer networks. . . ."[23]

The Combatant Commanders are the lead military designees responsible for implementing the operational plans specified by defense policy for their respective AORs. They need to be given all the proper direction and guidance possible so that when it is time to put together the strategic plan for execution, all the rules are clear and

[22] Alford, 27.

[23] Graham, A01.

precise. “Similar to strategic doctrine that has guided the use of nuclear weapons since World War II, the cyber-warfare guidance would establish the rules under which the United States would penetrate and disrupt foreign computer systems.”[24] Even though a positive step in the right direction, the guidance is apparently still rather generic. According to Richard A. Clarke, who recently resigned as special adviser to the president on cyberspace security, "We have capabilities, we have organizations; we do not yet have an elaborated strategy, doctrine, procedures."[25] This is apparent by the lack of specific components at the Combatant Commander level that deal with offensive cyber warfare. Currently, there are none at PACOM, and the staff was not even certain what was meant when asked about it.[26] STRATCOM is still getting used to its new command structure now that it has incorporated SPACECOM and all of the cyber duties associated with it. Coordination and specific delineations of responsibility are not as precise and streamlined as they could be. Due to this lack of very specific policy guidance and/or awareness, Combatant Commanders may be losing out on opportunities for offensive cyber attacks in their areas of responsibility. “Despite months of discussions involving principally the Pentagon, CIA, FBI and National Security Agency, officials say a number of issues remain far from resolved.”[27]

According to John Arquilla, associate professor of defense analysis at the Naval Postgraduate School and one of the leading authorities on cyber war, this is a very

[24] Ibid.

[25] Ibid.

[26] Bowen, interview by author.

[27] Graham, A01.

sensitive area that national security and military officials avoid talking about.[28] While Arquilla points out that offensive cyber tactics were employed in Kosovo to distort images generated by Serbian integrated air defense systems and proved essential to the high performance of the air campaign, such offensive tactics have not yet become the norm. Prior to conducting any type of offensive attack, of course, the President would be wise to gain public and congressional support for his initiative. Due to the ongoing war on terror, using any and all means of offensive warfare, to include cyber warfare, has already been suggested by this administration:

> In the last administration, there was a great concern about using techniques of cyber warfare that would then be emulated by others, and, by suggesting to the world that the Americans think this is a legitimate form of warfare, others might want to begin doing this as well. There was a great deal of concern about that. This administration is suggesting that we need to pull out all the stops to defeat terrorism. It is an admission, if only a tacit one, that cyberspace-based means of warfare are an essential part of the campaign against global terrorism.[29]

The United States should be mindful of setting a precedent of this nature and thus legitimizing offensive war as an acceptable new approach to warfare; however, it is a tool that should be used if properly employed while properly protecting our own assets. Besides, as Bruce Berkowitz has pointed out, ". . . anyone who uses lethal force today is being driven to similar tactics, because that is what works. The technology is so widely available that all countries will likely use network warfare in some form."[30] Al Qaeda resorted to using all forms of technology available to them in order to conduct the attacks on September 11 and probably would have used more if they had the capability to

[28] John Arquilla, "Cyber War," Frontline interview, 24 April 2003; available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html; Internet; accessed 2 January 2004.
[29] Ibid.

[30] Bruce Berkowitz, The New Face of War (New York, NY: The Free Press, 2003), 22.

infiltrate parts of our water system, power grid or nuclear reactor sites. Therefore, setting a precedent for this type of behavior is a moot point, since any enemy capable of employing these tactics will do so whether or not the United States chooses to go first.

## RECOMMENDATIONS

President Bush's new National Security Presidential Directive 16 is a step in the right direction. The basis of this direction should be used to establish specific rules of engagement so that the Combatant Commander can easily decipher and act upon the step by step instructions on how to properly conduct cyber warfare.

A recent Military Review article referred to U.S. cyber warfare policy as being "rudderless."[31] While this might be a bit exaggerated, it does draw attention to the fact that we need to follow up on National Security Presidential Directive 16 with a well-defined policy for both defensive and offensive cyber war, spelled out in a manner similar to *The National Security Strategy of the United States of America* or the *National Strategy for Combating Terrorism*. Once the policy has been clearly defined in such a document, cyber war should be elevated to something more than just a form of IO and given its own policies, procedures and rules of engagement.

In addition, a Joint Task Force should be formed to develop and direct offensive cyber war capabilities in accordance with the cyber war policy formulated in the strategy document discussed above. The Chairman of the JCS has mandated that by the year

---

[31] Byard Clemmons and Gary Brown. "Cyberwarfare; Ways, Warriors, and Weapons of Mass Destruction." Military Review 1 (September-October 1999): 42.

2005, every Regional Combat Command must have a Standing Joint Force Headquarters (SJFHQ).[32] This would be the perfect place to integrate a cyber warfare cell.

Since the Combatant Commander will not have authority to initiate offensive activities without clearance from the highest level of command, a centralized C2 agency at the level of the Joint Staff within the National Military Command Center needs to be put in place to facilitate coordination and rapid response with the SJFHQ cyber war experts in each region. This group should also be in charge of suggesting possible flexible deterrent options and standing rules of engagement in a Combatant Commander's AOR. Command structure and roles and responsibilities will need to be spelled out clearly in any overarching strategy document.

Due to the layout of current force structure with its multitude of responsible agencies, a single floating emergency response team should be developed as another resource to the Combatant Commander. This team should be devoted to implementing and protecting the defensive component of cyber war. The Combatant Commander could retain the same organizational approach as PACOM does, in which unit resources are used to respond to local criminal attacks (like hacking), but the Combatant Commander could call upon the floating emergency response team whenever it appears that the attack might be a threat to national security, rather than a criminal act. This team would be the "defensive" team, dealing with threats to national security and would have a common basis and understanding to coordinate with the same C2 agency located in the NMCC that already has direct coordination with the SJFHQ.

The bottom line is that Combatant Commanders should be given every possible warfare tool available to use for their own defense and offense. In order to define what

[32] Alberts and Hayes, 156.

cyber warfare tools are capable of providing the proper defense and offense, education, awareness training and indoctrination into this new form of possible attack needs to be conducted at the highest levels. This may prove to be the most difficult task, given that there are still numerous Services and agencies that still do their "own" individualized training and indoctrination and have their "own" defense methods to safeguard their "own" networks, thus creating continued interoperability problems. The prevalent form of current computer network attack scenarios for at least one Combatant Commander's AOR (PACOM) is still very defensive in nature, with information flow that sometimes is only one way communication with lack of feedback or follow on guidance to current computer attack fall out.

## CONCLUSION

Is cyber warfare more of a Ulysses Bow or Achilles Heel for the Combatant Commander? Some would argue that like Ulysses' Bow, cyber war is such a powerful weapon that only the United States, with its superior technology, can use it effectively as an offensive weapon, while others will argue that the very technological superiority that the United States enjoys has become an Achilles Heel in terms of vulnerability to cyber war tactics. Unfortunately for the Combatant Commander, current cyber war policy seems to be leaning towards the Achilles Heel as has been portrayed in the Eligible Receiver exercise and Moonlight Maze findings. These vulnerabilities, combined with lack of specific offensive guidance and procedures, leave the Combatant Commander with one less option for protecting his AOR. There are still numerous agencies, some only service related, that deal with cyber issues in different ways, and the reporting and feedback procedures between the Combatant Commanders and STRATCOM are still

being worked out. Even the subordinate structure within PACOM itself is still using different sets of rules and standards when dealing with cyber issues.

Prussian military theorist Carl Von Clausewitz claimed that, "Kind–hearted people might of course think there was some ingenious way to disarm or defeat an enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed: . . ."[33] Today, this viewpoint no longer describes the full spectrum of modern warfare. The United States currently has the technology to initiate war without the use of force and possibly prevail without bloodshed. It is time to re-examine our traditional way of thinking and use the technology we have available in order to "subdue our enemy without fighting," Sun Tzu's acme of skill.

In order for a Combatant Commander to use his technological "Ulysses Bow," exact guidelines, streamlined command and control, national policy and rules of engagement need to be formulated and well understood. Cyber warfare may be one of the greatest threats that nations have ever faced, especially the United States, since we are the most technologically advanced and are heavily dependent on our computer based infrastructure. Therefore, defensive computer operations are still in the forefront in our current military organizations and forethought. Defense is certainly the first step in ensuring the Combatant Commanders "Achilles heel" is well protected, but it is time to start using all available forms of warfare at our disposal. Just as it calls for pre-emptive attacks if necessary, our National Security Strategy should include all cyber warfare

[33] Carl Von Clausewitz, On War. Book I, translated by Michael Howard and Peter Paret. (Princeton, NJ: Princeton University Press, 1976) 75.

capabilities as well, thus supplementing existing non-lethal methods of attack in the Combatant Commanders' tool box.

## Selected Bibliography


Alberts, David S., and Richard E. Hayes. Power to the Edge: Command, Control in the Information Age. With a Foreword by John Stenbit. Washington, D.C.: Command Control Research Program, DoD, June 2003.

Alford, Lionel D. "Cyber-Warfare: A New Doctrine and Taxonomy." CrossTalk 14, no.4 (April 2001): 27-30; available from http://www.stsc.hill.af.mil/crosstalk/2001/04/alford.html; Internet; accessed 22 December 2003.

Are, David C. "When Does the 'Hacker' become an 'Attacker'?" Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1998.

Arquilla, John. "Cyber War." Frontline interview. 24 April 2003; available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html; Internet; accessed 2 January 2004.

_____. "Moonlight Maze" Cyber war Frontline. 24 April 2003; available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/; Internet; accessed 27 December 2003.

Berkowitz, Bruce. The New Face of War. New York, NY: The Free Press, 2003.

Bowen, Calvert L. Interview by author, email, United States Pacific Command, HI., 6 January 2004.

Brand, Gary. "Protecting the United States Against Information Warfare." Carlisle Barracks, PA: U.S. Army War College, 1 April 2000.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Gooden, eds. "Cyberwar: Security, Strategy, and Conflict in the Information Age." Fairfax, VA: AFCEA International Press, May 1996.

Chairman of the Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington, D.C.: U.S. Government Printing Office, 1997.

_____ . Joint Doctrine for Information Operations. Joint Pub 3.13. Washington, D.C.: U.S. Government Printing Office, October 9, 1998.

_____ . Joint Vision 2020: America's Military Preparing for Tomorrow. Washington, D.C.: U.S. Government Printing Office, 2000.

_____ . Joint Doctrine for Command and Control Warfare. Joint

Pub 3.13.1. Washington, D.C.: U.S. Government Printing Office, 6 February 1996.

Christensen, John. "Bracing for Guerrilla Warfare in Cyberspace." CNN Interactive. April 6, 1999; available from http://edition.cnn.com/TECH/specials/hackers/cyberterror/; Internet; accessed 28 November 2003.

Clemmons, Byard, and Gary Brown. "Cyberwarfare: Ways, Warriors, and Weapons of Mass Destruction." Military Review 1 (September-October 1999): 35-45.

CSIS Global Organized Crime Project. Cybercrime—Cyberterrorism—Cyberwarfare—Averting an Electronic Waterloo Washington, D.C.: Center for Strategic and International Studies, 1998.

Dorobek, Christopher J. "Navy Creates Network Command." Federal Computer Week March 27, 2002. < http://www.fcw.com/fcw/articles/2002/0325/web-navy-03-27-02.asp; Internet; accessed 27 December 2003.

Goldberg, Ivan. Institute for Advanced Study of Information Warfare (IASIW) October 27, 2003. http://www.psycom.net/iwar.1.html; Internet; accessed 3 January 2004.

Graham, Bradley. "Bush Orders Guidelines for Cyber-Warfare." Washington Post, February 7, 2003.

Hamre, John. J. "Counter-Proliferation Efforts Must Include Defense Against Cyber Attacks." Defenselink, June 22, 1998.

_____. "Eligible Receiver" Cyber war Frontline. 24 April 2003; available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/; Internet; accessed 2 January 2004.

Joint Command Control and Information Warfare Staff. Information Operations: The Hard Reality of Soft Power, Norfolk, VA: Joint Forces Staff College, 2000.

Sun Tzu. The Art of War. Translated and with an introduction by Samuel B.Griffith. New York: Oxford University Press, 1971.

"U.S. Military Grapples with Cyber Warfare Rules." Reuters, Monday 8 November 1999; available from http://www.hartford-hwp.com/archives/27a/021.html; Internet; accessed 26 January 2004

United States Strategic Command webpage: "Joint Task Force – Computer Network Operations." Fact Sheet, February 2003; available from

http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm; Internet; accessed 29 November 2003.

Von Clausewitz, Carl. On War. Translated by Michael Howard and Peter Paret. Princeton, NJ: University Press, 1976.