STRATEGY RESEARCH PROJECT

THE ROLE OF ARMY SPECIAL OPERATIONS FORCES IN INFORMATION WARFARE IN THE 21ST CENTURY

BY

LIEUTENANT COLONEL JOHN H. BONE, JR.
United States Army

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

The Role of Army Special Operations Forces in Information Warfare in the 21st Century

by

LTC John H. Bone, Jr.
United States Army

COL (RET) Robert Coon
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: John H. Bone, Jr.

TITLE: The Role of Army Special Operations Forces in Information Warfare in the 21st Century

FORMAT: Strategy Research Project

DATE: 10 April 2000 PAGES: 20 CLASSIFICATION: Unclassified

Relevancy on tomorrow's battlefield begins today. The United States military is facing an amorphic future. There is a lack of a clearly definable enemy. The nation's leadership has employed the military on more contingency operations during the last ten years than the prior fifty. General Schoomaker, Commander in Chief, U.S. Special Operations Command, has been emphasizing self-examination as it pertains to emerging missions and force structure since 1997. Maintaining a relevancy into the future is critical if ARSOF is to remain an effective weapon to help maintain America's freedom. This paper reviews the seven forms of information warfare and suggests four potential information warfare mission capabilities that could be added to the ARSOF mission matrix. These potential mission profiles are compatible with existing mission matrixes under the capabilities of Psychological Operations, Direct Action, Special Reconnaissance and Foreign Internal Defense. The decision to develop and incorporate the new skill sets rests with the Leadership of SOF in conjunction with current information warfare policy and NCA guidance.

TABLE OF CONTENTS

THE ROLE OF ARMY SPECIAL OPERATIONS FORCES IN INFORMATION WARFARE IN THE 21ST CENTURY

> We must look toward the future with anxious, wide-open eyes to steel ourselves for what may come, so that the reality may not take us by surprise. This is all the more necessary in the revolutionary period we are living through-so much so that he who is not ready will have no time to get ready or to correct the errors of the past.
>
> —Giulio Douhet

We have entered the 21st Century at the speed of light. Not only are we seeing expediential increases in technology but also in asymmetrical threats to the United States. Today we have more service men and women conducting operations world wide than during the previous fifty years. These deployments are not the traditional deployments to support the vital national interests of the United States as portrayed during the cold war. Rather, they are supporting national policy of the day as identified by the political leadership of the nation. These interests include providing humanitarian assistance and disaster relief, peacekeeping, peacemaking and maintaining the ability to fight and win in two major theaters of war. We are engaged on a battlefield which is asymmetric in nature. We are already under computer attack ranging from hackers disrupting email to stealing money from on line purchases to planting viruses in business and military computers. The Army is struggling with the concept of who or even what is the enemy we must prepare for if we are able to fight and win our nation's battles. There are a number of writings on the subject of informational warfare with some key observations being:

> —The effects of the new-world order are not yet totally understood; vulnerability and risk are not as easily defined as they were during the cold war. [1]
>
> —Applying this concept (...interdependency and vulnerability...) to the elements of national power implies that leaders at all levels share an increasingly common view of the situation. The lines between tactical, operational, and strategic decision-making blur and create opportunities for flattening standard decision making structures.[2]
>
> —The concept (...informational warfare...) is rooted in the indisputable fact that information and information technologies are increasingly important to the national security in general and to warfare specifically. According to this concept, advanced conflict will increasingly be characterized by the struggle over information systems[3]

This phenomenon calls for paradigm shifts in National Security Strategy, National Military Strategy as well as adaptation by the Army. The Chief of Staff of the Army, General Shinseki, has begun this revolution. In a speech given 12 October 1999 to the Sergeants Major of the Army, he directed the development of forces which are responsive, deployable, agile, versatile, lethal, survivable and sustainable. He stressed the Army's need to maintain strategic dominance across the entire spectrum of operations.[4] Similarly, General Schoomaker, Commander in Chief, U.S. Special Operations Command, (CINSOC), while serving as the Commanding General of the U.S. Army Special Operations Command, (USASOC), in February 1997 told his Commanders "Too many times we get trapped by the tendency to

"make yesterday perfect" and miss the really strategic opportunities we have to leap into and beyond tomorrow's challenges." [5] The senior leadership's recognition of the increased importance of information warfare drives subordinates to rethink how to conduct operations, adjust force structure and employ forces.

U.S. Army Special Operations Forces (ARSOF) have been serving the leadership of our nation as a strategic economy of force asset. ARSOF has supported the National Command Authority (NCA) and regional Commanders in Chief (CINCs) with peacetime engagement focused on preventing conflict, humanitarian assistance and the ability to quickly transition to combat operations.[6] This paper will examine the seven forms of informational warfare, followed by an examination of potential roles of ARSOF to ensure their relevancy to the NCA and regional CINCs on the information battlefield. I want to stress that the ideas and opinions concerning future information warfare and ARSOF's role in it are strictly my own and do not reflect current or projected U.S. policy.

INFORMATION WARFARE

What is information warfare? Is it a sole function of computers and their associated technologies or is it something more amorphic? Martin C. Libicki categorizes information warfare as real, arguable, potential and unlikely warfare.[7] It must be noted up front that of the seven forms of informational warfare the final three forms: hacker warfare, economic information warfare and cyber warfare bleed over into one another and are contentious issues for the United States today. Much of U.S. policy concerning these three forms of information warfare is classified and will not be addressed in this paper.

Command and Control Warfare (C2W)

Command and Control Warfare is as old as the conduct of war. Armies have always sought to separate the enemy's leader form his men to render the enemy floundering about the battlefield without direction. Anti-head or decapitation is the first of the two forms of C2W. It is simply depriving a leader of the means to communicate with his subordinates. Normally this means the destruction of the enemy's command post or his communications capability. The evolution of communications equipment reduces the signature of these high pay off targets. Today you can remote antennas, mask communications gear by electronic clutter and reduce the traffic flow to headquarters by video or teleconferencing. These techniques and other future techniques will increase the difficulties of addressing these high pay off targets.

The second form of C2W is called anti-neck or networks attack. This form of warfare concentrates on reducing the communications networks available to the enemy. These operations are designed to surgically separate the commanders from their units both vertically and horizontally. This type of attack allows the denial of battlespace to the enemy by preventing communications within both offensive and defensive areas of operation. It gives the commander the opportunity to shape the battlefield possibly without a great expenditure of men or munitions in order to create exploitable vulnerabilities.

Intelligence – Based Warfare (IBW)

Intelligence-Based Warfare is the direct feed of intelligence into the operations to provide real time knowledge of the enemy's disposition. It provides the information needed to execute the decide, detect and deliver methodology for employing weapons to destroy the enemy. This methodology identifies which targets are important (decide), identifies where they are on the battlefield (detect), and what weapon system is appropriate for the mission. IBW is no longer the approximation of the enemy and his intentions; it is an assimilation of the electronic input from collection platforms which electronically survey the battlefield. Technological innovations provide a venue by which signal intelligence, imagery intelligence and human intelligence can be fused, disseminated and acted upon by the commanders in a fraction of time. IBW is both offensive and defensive in nature and often utilizes the same technical systems. Albeit there are some systems which lend themselves to one or the other employment. For instance JSTARs while capable of identifying movement cannot, without sensors being placed on friendly vehicles, identify friend from foe or the type of vehicle. During offensive operations the JSTARs capability gives the commander highly accurate intelligence of the enemy's movements until both sides become engaged in the close battle. At this time relevancy is reduced until one side or the other emerges and continues its operations. During defensive operations JSTARs is exceptional for identifying attacking and supporting forces which is then translates into deep attack information for the defending commander.

Electronic Warfare (EW)

The third form of Information Warfare is electronic warfare. Unlike the previous two forms of IW that focus on systems, EW is operational in nature directed at degrading the enemy's radioelectronic and cryptographic abilities. This is becoming an increasingly more important facet of IW as "... 90% of the U.S. Armed forces' communications, for example, flow over commercial channels."[8] Needless to say that attacks upon these systems will increase civilian causality rates as the traditional noncombatants are now without telecommunications networks and computer networks designed to run the national infrastructure and support businesses. This brings a whole new dimension to the battlefield as the political and military leaders must now face pressure from the civilians to restore these affected systems.

EW attacks upon these systems by the traditional methods of jamming or targeting for destruction create issues of international proportion. The destruction of communications or global positioning satellites would impact multiple nations as the commercialization of space continues. We are seeing nations without the technology to launch satellites renting space telecommunications capabilities from corporations that have pooled their resources for the commercial venture. If the multinational corporate owners of these space telecommunications systems are neutral in the next conflict, the use of political or economic persuasion may be the weapons of choice in order to blind or deny access to the satellite by the enemy. The destruction of transnational, commercial, space platforms has the potential to create thousands of real (due to the downing of a global positioning satellite) or electronically (affecting business networks) causalities. This type of offensive operation would result in unacceptable consequences i.e. the loss of world support for the executing nation.

The second facet of EW is cryptography or the encoding of message traffic. Unlike the previous years, in which the U.S. enjoyed the ability to break, read and act upon the enemy's message traffic, the advent of the triple-digital encryption standard and the use of public and private key encryption will shortly overwhelm the capabilities of the code breaking computers. These systems coupled with spread-spectrum and frequency hopping communications equipment will virtually eliminate the ability of computers to break enemy's' codes in the near future.[9]

Psychological Warfare

Psychological warfare, or as is it more commonly referred to - PSYOPS, is the inducement and re-enforcement of foreign attitudes and behavior favorable to the originator's objectives[10] These operations are divided into four subcategories: operations against the national will, operations against opposing commanders, operations against troops, and cultural conflict. These are preplanned operations that require vetting and approval from the National Command Authority for implementation. The operations must be as factual as possible if they are to affect the target audience. If the PSYOPS campaign is perceived as propaganda or out right lies then the operations will be ineffective.

The most effective and possibly the most potent of the four sub categories is the cultural conflict. The U.S. is daily engaged in the spread of our culture around the world. We market our products like Coke a Cola and Levies worldwide. Inbeded in each advertisement is the feel good, American way of life. This message is so strong that some countries try to outlaw our products from import. America sees this as an infringement upon free trade and rejects the band accordingly. However, what we are indirectly doing is preparing the battlefields for future operations against the national will.

National will is quite simply the willingness of the majority of a nation to believe and support the actions currently undertaken by their political leadership. The undermining of this foundation for the conduct of operations against another nation could very simply end the conflict. Probably the most well known example of national will was the loss of the Viet Nam war. Regardless of the victories on the battlefield the people were extensively affected by the propaganda campaign North Viet Nam waged in the American press. The Viet Namese PHYSOPS message to the American people was - the war was beyond their ability to win. The end state of the PHYSOPS operation was the withdrawal of American forces from South Viet Nam and its capitulation in the mid 70s. National will may be expressed through a political process or through the conduct of limited violent rejection of the nation's policy.

The decline of the national will is but one facet of the PSYOPS focused against the opposing commander. These operations are designed to disorient, confuse, and introduce unexpected variables into commander's decision cycle. These operations may include the conduct of deception operations or the infusion of misinformation into the telecommunications network which affects the commander's situational awareness of ongoing events both within the military arena and within the civilian world. Regardless, once a commander looses effectiveness in making decisions due to misinformation, disorientation or becoming overwhelmed by unexpected events the initiative rests with the aggressor.

The final subcategory of PSYOPS is operations against troops. This is quite simply focusing information to the soldiers on the ground in an attempt to demoralize them so they will not fight. This can be accomplished through a myriad of ways such as undermining the soldiers' confidence in their leaders' military competencies or fostering doubt in the soldiers concerning his commander's motivation for the conduct of the war. Soldiers will fight for many reasons, but there has to be some legitimacy to the cause. Simply furthering the personal agenda of the commander without some trickle down effect, (e.g. improving the lot of the nation), does not inspire soldiers to give their lives in support of that commander's agenda. Another technique is to convince the enemy that he will be overwhelmed by firepower and resistance is useless. Once the soldiers' morale is defeated the conflict will terminate in relatively short order under the pressure of offensive operations.

Hacker Warfare

Hacker warfare is the cyber attack on a computer network with the intent to create a range of problems or to collect information. These attacks are categorized as total paralysis, intermittent shutdown, random data errors, illicit systems monitoring and intelligence collection, and injection of false message traffic.[11] Even the stealing of services, normally associated with the civilian sector, can apply in regards to requesting increased production of critical weapon or system components. An enemy may want to deprive the opponent of a resource so the critical component cannot be produced.

Hacker warfare, a component of computer network attack (CNA), is a highly contentious issue. The ramifications of conducting computer attacks is not clearly understood from the nation state perspective. This is an especially lucrative venue to terrorists or rogue states who do not fear retalliation. The issue pivots around the ability of a sovereign state to comprehensively protect its systems, ensuring their operations are protected from hackers. The aggressor employs malicious software such as viruses, logic bombs, Trojan horses, worms and sniffers. Until this issue is either resolved or at least the effects can be ameliorated the policy discussions and decisions will remain highly classified. Yet, I would be remiss if I did not address this issue in at least a generic manner.

Economic Information Warfare (EIW)

This type of offensive operation is a hybrid of the traditional blockade of the imports and exports. This operation focuses on blockading information, monetary transactions and information about the industrial markets vice the traditional transportation of goods. The ability of a sovereign nation or even the United Nations to impose information blockades as part of prehostilities and during hostilities could very well be more effective than naval blockades designed to prevent the introduction of silkworm into the theater of operations. Here again the initiating player must protect his own systems. Turning off the monetary transactions of a nation would lead to disaster in a very short period of time. A country unable to handle its international debts would quickly loose the ability to provide for survival of its people and businesses. Denying information to competitors thereby reducing their effectiveness is research, product development and competitiveness in the market is another example of a slower but no less effective means to cripple or terminate a hostile nation's aggression.

Cyber Warfare

This is the seventh form of informational warfare. It contains two sub categories: information terrorism and semantic attack.[12] Information terrorism attacks information in data- bases in an effort to gain information that may be used for blackmail or altered to produce embarrassment to the target. This may be effective only because of the time, effort and resources tied up correcting the erroneous data entries. A semantic attack against an operating system is designed to make it appear to be operating correctly. In reality, the computer is generating answers with unacceptable variances by generating bad decisions or failed execution. An example of semantic attack could be the adjustment of coordinates relayed to a cruse missile causing it to miss the intended target striking harmlessly into an uninhabited area.

ARSOF INTRODUCTION

The seven forms of information warfare present a picture of a wide-open operational arena. This is an arena in which, if the U.S. is not proactive in its program of offensive and defensive contingencies, it can fall victim to another nation's information warfare. This is a danger because the cost of technology is becoming more affordable and the cost of raising and maintaining a conventional military is becoming unaffordable. Enemies that invest the preponderance of their defense budgets into information warfare vice conventional forces may one day pose creditable threats, capable of detering the United States' ability to impliment its foreign policy objectives within the region. Many of the elements of information warfare are better executed at the national level. The proximity to the policy decision-makers, accessibility to abundant hardware options, and multiple entry points to the information super highway renders it virtually unnecessary to prosecute IW from outside the United States. However, there are opportunities that lend themselves to conducting IW from within the theater of war or from another area of operation.

Force projection operations, in support of foreign policy considerations, have involved the U.S. military in peace keeping, peace enforcement and humanitarian assistance at an unprecedented rate. Concurrently the military must maintain trained and ready forces, capable of executing two major theaters of war simultaneously. ARSOF is but one component of the U.S. force structure. It has played a significant role in the execution of American Foreign Policy. Although these operations are often executed at the tactical level, they have at least operational and normally strategic impact on the current operation. ARSFO possesses unique capabilities distilled from their unconventional training and equipment, out of the box solutions to problems, and ability to understand the political ramifications of their operations. These characteristics make ARSOF ideal to operate on the information battlefield in certain capacities. AROSF forces include the 75th Ranger Regiment, 160th Special Operations Aviation Regiment, U.S. Army Special Forces, Psychological Operations and Civil Affairs units. The remainder of

this paper will address the ARSOF capabilities and possible roles for their employment in the conduct of either offensive or defensive informational warfare.

Joint Pub. 3-13 provides unclassified definitions for both offensive and defensive information operations that must be kept in mind when discussing the future roles of ARSOF on the information battlefield.

> Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision-makers and achieve or promote specific objectives. These supporting capabilities are activities that include, but are not limited to, operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and may include computer network attack.[13]

> Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted through information assurance, OPSEC, physical security, counterintelligence, EW, and SIO. Defensive IO ensure timely, accurate and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Offensive IO also can support defensive IO.[14]

Psychological Operations

PSYOPS is and will probably remain the largest contribution that ARSOF makes on the information warfare battlefield. PSYOPS will continue to address the four previously mentioned subcategories of operations against the national will, operations against opposing commanders, operations against troops and cultural conflict. PSYOPS brings a number of non-lethal weapon systems to the fight.

First is the use of EC-130 Commando Solo aircraft. This aircraft possesses AM, FM, HF TV and military communications bands capabilities as well as secure teletype to support the electronic transmission of information designed to influence foreign nation attitudes. This platform was used extensively during Desert Shield/Storm to help convince Iraqi soldiers that resistance was futile. Unfortunately, the electronics on board are outdated and must be replaced in order to maintain relevancy in the future. The TV and radio broadcast bands are far too restrictive for future operations. The platform lacks the ability to broadcast real time TV and radio infomercials and news updates. Currently the PSYOPS Dissemination Battalion must produce pre-recorded material for the EC-130 to transmit during flights. There is the need to develop a satellite ground to air link capability to allow for the real time transmissions to take place.[15]

The Dissemination Battalion also possesses audiovisual, printed material production, signal support and media broadcast capabilities. However, there is a lack of ability to tap into cable TV systems. This capability could increase access to the civilian and military target audiences. The battalion currently possesses a limited ability to produce web pages for those interested. The problem with this method is obvious, only those who choose to log on to the web page are going to be exposed to the PSYOPS campaign. The development of a computer hacker capability to enter into the enemy's news service

computer system could make information significantly more accessible to the target audience. This concept could also be applied to intrusion of the civilian email networks. The ability to send messages directly to the political leadership, family or friends of the enemy through the civilian email system offers a precision targeting mechanism. Another dimension of hacking into civilian email is achieved when the attacker disguises himself as a known and trusted source. Execution of operations in this vernacular equates to the conduct of clandestine operations. This provides the U.S. with the ability to use intelligence regarding personal behavior, financial, and political compromises to elect a desired outcome.

Direct Action (DA)

Direct Action is "the conduct of operations to seize, damage, or destroy a target, capture or recover personnel or material in support of strategic/operational objectives or conventional forces."[16] ARSOF, especially Special Forces (SF), is well suited for the conduct of information warfare as part of clandestine or covert, pre-hostility cross border operations as well as deep operations upon the commencement of hostilities. Normally, SF Operational Detachments-Alpha (ODA) will operate as part of the deep battle in the conduct of DA operations. These operations may include the targeting of C2 centers in support of C2W anti-neck operations. Increasingly C2 operations are reducing or eliminate electronic signatures by offloading antennas many miles from the C2 node, laying fiber cables, masking communications emissions with electronic clutter, and utilizing dispersed photovolatic collectors to produce electricity. These efforts may, in effect, render the C2 center indistinguishable utilizing traditional electronic intelligence templates. This may require a deep infiltration of personnel into the enemy's rear area to locate the C2 center and then neutralize it by a means that support the commander's scheme of maneuver. This means attacking a sub-component of the C2 center by a weapon system that renders the system destroyed, disabled for a limited period of time or affected by a semantic attack that desynchronizes the enemy's efforts to conduct combat operations.

An ODA trained in information warfare may chose from a menu of weapon systems to conduct the attack. These weapons include standard laser designators to mark the target for attack by smart munitions, a directed energy weapon to destroy the micro chips of the C2 computer system, or the introduction of malicious software to paralyze, shutdown, inject false message traffic or even generate random data errors. The first two methods are well within the current or near future technological capabilities. The third requires the development of computer hacker skills as well as the ability to conduct cable intrusion into the C2 hard line system. It must be recognized that the sophistication of CND will most probably immediately identify the cable intrusion. In response to this threat the enemy will apply defensive operations that disrupt, degrade or turn off the CN and in effect help accomplish the attacker's objective.

Another DA mission could be the recovery of a functioning piece of equipment. This could be a computer, encrypting equipment or even the equipment used to electronically mask communications emissions. This type of operation falls well within the existing capabilities of ARSOF to conduct long range infiltration, fire support and extraction operations as forces are currently configured.

Special Reconnaissance (SR)

The conduct of these operations is "to obtain or verify, through visual observation or other collection methods, information concerning enemy capabilities, intentions, and activities in support of strategic/operational objectives or conventional forces."[17] If the U.S. is successful in blinding or degrading the enemy's space based telecommunications systems the enemy may use systems of communication that we may not be able to intercept. This inability to collect could be attributed to any number of considerations (e.g. the operational theater may contain mountainous terrain that could mask low powered systems). Small Scale Contingencies or even the threat of a Major Theater War could prioritize the national systems to other theaters of operations. Limited theater EW assets may not possess the capabilities to reach the area of interest. Over flight rights could be denied by neighboring countries desiring to maintain neutrality. Any of these possibilities would not hinder the use of ODAs to penetrate enemy airspace and conduct a signals intelligence operation. Current equipment would have to be updated, lightened and capabilities improved for this to become viable beyond the current force protection effort of the Special Operations Teams – As (SOT-A).

The U.S. could employ cheap sensors and electronic clutter devices to determine enemy movements, degrade their communications and fire control networks or even monitor their stockpiles of Weapons of Mass Destruction (WMD). At first glance the use of aerial delivery might seem most appropriate because of the speed of execution, the ability to deploy large payloads and the unprecedented successes of recent air campaigns. However, it is conceivable that the commander may want to ensure the enemy is unaware of monitoring efforts. Infiltration of an ODA utilizing a stand-off scenario to inplace the sensors is a viable option. This is especially true of a scenario involving the movement of a WMD from its storage to staging area. An ODA with real time video capability, once alerted by the sensors of activity or the presence of chemical traces, can video the event which could then be used to dissuade the enemy from using the WMD, leverage neutral nations to support the U.S. efforts or help to fractionate the enemy alliance.

Foreign Internal Defense (FID)

The U.S. maintains contacts with many nations through the Security Assistance Program. This program is the impetus for the worldwide FID operations conducted by ARSOF. These operations are "...designed to assist another government in any action taken to free and protect its society from subversion, lawlessness and insurgency."[18] The conduct of CNA against either the host nation of a FID mission, (possibly to infect their CN or activate malicious software), or to use it as the base of operations for the conduct of CNA against an enemy falls into the realm of clandestine and covert operations.

It is certainly possible that U.S. may decide to conduct preemptive operations against an enemy in order to ensure the security of U.S. vital interests. ARSOF routinely provides the Host Nation with stay-behind training packages to enable the Host Nation to sustain its trained operational capabilities. Computer diskettes containing training information could contain malicious software. It is even

conceivable that diskettes could be purposely left behind for the intended purpose of the Host Nation infecting their own system with malicious software. It is also possible for a hacker to utilize the local telecommunications hard lines to hack into the Host Nation's computer networks.

CONCLUSION

The United States will continually reexamine its policies in response to the changing threats, technological innovations and international agreements that affect this battlefield. The Chief of Staff of the Army is leading the change of the conventional Army with the creation of medium brigades capable of operating across the spectrum of Military Operations Other than War in response to the changing world. As previously mentioned, General Schoomaker has challenged ARSOF to conduct self-assessments regarding emergent missions and capabilities. ARSOF must identify and develop information warfare roles and capabilities as part of the NCA and Theater CINCs' arsenal of operational and strategic information warfare assets.

To that end this paper has identified four forms of information warfare, PHYSOPS, C2W, Hacker Warfare and Cyber Warfare that suite ARSOF to execute in the future. These forms of IW have been addressed as part of the ARSOF mission paradigm under the capabilities to execute PHYSOPS, DA, SR and FID operations. None of these capabilities represent radical ideas and in fact often mirror IW operations currently being conducted against the United States. The decision to begin resourcing and training these identified capabilities will rest with SOF leadership.

WORD COUNT = 4810

ENDNOTES

[1] Stephen Klinefelter, National Security Strategy and Information Warfare, Strategy Research Project, (Carlisle Barracks, U.S. Army War College, 23 July 1997), 2 – 4.

[2] Douglas A. MacGregor, "Future Battle: The Merging Levels of War," Parameters 22 (Winter 1992-93): 33-47.

[3] Martin C. Libicki, "What is Information Warfare?" Center for Adnance concepts and Technology Institute for National Strategic Studies, National Defense University,(August 1995): ix.

[4] General Eric K. Shinseki, "The Army Vision: Soldiers On Point for the Nation . . . Persuasive in Peace, Invincible in War," 12 October 1999; available from <http:/www.hqda.army.mil/ocsa/chief.htm>; Internet; accessed 10 February 2000.

[5] LTG Peter J. Schoomaker, "Professional Development." Memorandum for USASOC Commanders, Fort Bragg, NC,3 February 1997.

[6] Peter J. Schoomaker, Special Operations Forces: the Way Ahead, Position Paper, (United States Special Operations Command, MacDill AFB, FL: 1998), 2-3.

[7] Libicki, 85.

[8] Thomas G. Mahnken, "War and Culture in the Information Age," Strategic Review (Winter 2000): 42.

[9] Libicki, 32.

[10] Office of the Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, (Washington, D.C.: U.S. Department of Defense, 1 February 1995),III-31.

[11] Libicki, 49-50.

[12] Libicki, 75-77.

[13] Office of the Joint Chiefs of Staff, Joint Doctrine for Information Warfare, Joint Pub 3-13, (Washington, D.C.: U.S. Department of Defense, 9 October 1998), viii.

[14] Ibid.

[15] The ideas in this paragraph are based on remarks made by a speaker participating in the Commandant's Lecture Series.

[16] Chairman, Joint Chiefs of Staff, Joint Doctrine for Special Operations, Joint Publication 3-05, (Washington, D.C,: U.S. Joint Chiefs of Staff, 17 April 1998), 10-11.

[17] Ibid.

[18] Ibid., 11.

BIBLIOGRAPHY

Chairman, Joint Chiefs of Staff. Joint doctrine for Military Operations Other Than War. Joint Pub 3-07. Washington, D.C., U.S. Joint Chiefs of Staff, 16 June 1995.

Chairman, Joint Chiefs of Staff. Joint Doctrine for Special Operations. Joint Publication 3-05. Washington, D.C,: U.S. Joint Chiefs of Staff, 17 April 1998.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1998.

Commander. United States Special Operations Connamd. Special Operations in Peace and War. USSOCOM Pub 1. McDill AFB, Tampa FL. 25 January 1996.

Douhet, Giulio. "The Command of The Air." In Roots of Strategy, Book 4, ed. David Jablonsky, 265-407. Manchanicsburg: Stackpole Books, 1999.

Flake III, Jackson L. ForceXXI and Beyond: Bridging the Combat Power Gap with Fires. Strategic Research Project. Carlisle Barracks. U.S. Army War College. 6 April 1998.

Fredricks, Brian F. "Information Warfare at the Crossroads." Joint Forces Quarterly (Summer 1997): 97-103.

Information Assurance. Legal, Regulatory, Policy and Organization Conciderations. 4th Edition. August 1999. Available from <www.dtic.mil/jcs/j6/j6k/ia.pdf>. Internet. Accessed 15 March 2000.

Klinefelter, Steven. National Security Strategy and Information Warfare, Strategy Research Project, Carlisle Barracks, U.S. Army War College, 23 July 1997.

La Perla, Philip A. Creating information Knowledgeable Leaders Through Information Operations Education. Strategic Research Project. Carlisle Barracks. U.S. Army War College. 1 April 1998.

Libicki, Martin C. "What is Information Warfare?" Center for Advance Concepts and Technology Institute for National Strategic Studies, National Defense University, (August 1995).

MacGregor, Douglas A. "Future Battle: The Merging Levels of War," Parameters 22 (Winter 1992-93): 33-47.

Mahnken, Thomas G. "War and Culture in the Information Age," Strategic Review (Winter 2000): 40-46.

Office of the Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington, D.C.: U.S. Department of Defense, 1 February 1995.

Office of the Joint Chiefs of Staff. Joint Doctrine for Information Warfare. Joint Pub 3-13. Washington, D.C.: U.S. Department of Defense, 9 October 1998.

Schoomaker, Peter J. "Professional Development." Memorandum for USASOC Commanders. Fort Bragg, NC,3 February 1997.

Schoomaker, Peter J. Special Operations Forces: the Way Ahead, Position Paper. United States Special Operations Command, MacDill AFB, FL: 1998.

Schwartau, Winn. Information Warfare. New York: Thunder's Mouth Press, 1994.

Shalikashvili, John M. Joint Vision 2010. Washington D.C.: Joint Chiefs of [19]Staff. 1996.

Shinseki, Eric K. "The Army Vision: Soldiers On Point for the Nation . . . Persuasive in Peace, Invincible in War." 12 October 1999. Available from <http:/www.hqda.army.mil/ocsa/chief.htm>; Internet; Accessed 10 February 2000.

Stewart, Michael J. Information Operations, Information Warfare: Policy Perspectives and Implications for the Froce. Strategic Research Project. Carlisle Barracks. U.S. Army War College. 15 April 1997.