STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: A LAYMAN'S PERSPECTIVE

BY

LIEUTENANT COLONEL ROY V. BISHOP
United States Army

USAWC CLASS OF 1997

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

UNCLASSIFIED

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: A LAYMAN'S PERSPECTIVE

by

LIEUTENANT COLONEL ROY V. BISHOP

UNITED STATES ARMY

COLONEL MORRIS E. PRICE, JR.

PROJECT ADVISOR

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

UNCLASSIFIED

ABSTRACT

AUTHOR: Roy V. Bishop (LTC), USA

TITLE: Information Operations: A Layman's Perspective

FORMAT: Strategy Research Project

DATE: 1 April 1997 PAGES: 30 CLASSIFICATION: Unclassified

The subject of Information Operations (IO), formerly called Information Warfare, is having a profound impact on the Department of Defense and the Armed Services because of the proliferation of information technologies throughout the Armed Services. Most literature on the subject will tell you that IO is the center piece for a larger Revolution in Military Affairs. Whether these technological innovations represent a revolution or not, is of little importance in the grand scheme of things. But taking maximum advantage of there potential is. Utilization of these technologies is not without considerable risk. This paper examines where we got started with incorporating high technology into intelligence, weapons, and command, control, communications and computer systems, assess where we are and where we are going, discuss the associated vulnerabilities and what we are doing to protect against them.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

INTRODUCTION

"Information Warfare will dominate 21st century conflict. Although information warfare is not unique to the Information Age, the exponential growth in information technologies during the past few decades has engendered heretofore unheard of opportunities for information exploitation. Properly conceived information warfare operations can be inexpensive, highly effective and executed by almost anyone anywhere. Achieving information dominance over an adversary will decide conflicts long before resort to more violent forms of warfare is necessary".

Daniel E. Magsig
Information Warfare In the Information Age

As a result of the end of the Cold War and the implosion of the Soviet Union, there are many profound arguments concerning the future of the military services that have yet to be decided. Since 1991, there has been a 24 percent reduction in force strength and a 38 percent reduction in the budget after adjustments for inflation.[1] Can the Armed forces absorb farther cuts in manpower and the budget? Can technology make up the difference freeing funds reaped from the Cold War's end that can be applied to other segments of the Nation's economy?

Identical to the aftermath of every major conflict in this nation's history, we have to decide where do we go from here, considering the United States' position in world leadership and potential threats to the United States and our Allies. Regardless of the outcome of these arguments, one thing has become certain. The future Armed Services of the United States will be outfitted with the most technologically advanced equipment that the Information Age can provide. One only needs to look at what was achieved and how it was achieved

in our most recent major conflict in the Persian Gulf and lesser military actions, such as Haiti and Bosnia, to know that utilization of silicon based technologies will be the wave of the future. These technologies already bring significant advantages to military commanders in the realm of Dominant Battlespace Knowledge (DBK). "DBK involves everything from automated target recognition to knowledge of an opponent's operational scheme and the networks relied on to pursue that scheme. The result of achieving DBK will be an increasing gap between the United States military forces and any opponent in awareness and understanding of everything of military significance in any area in which we may be engaged."[2]

The original intent of utilizing existing and emerging information technologies was to enhance warfighting capabilities by providing commanders with better integration of weapons systems and a better way to employ them to maximize their potential, but not as a substitute for force structure. This paper will examine how the Armed Services got started along this path, where we are heading, and will address the significant of technologies to warfighting, vulnerabilities, and some of the hurdles to be overcome.

BACKGROUND

Where did the quest for silicon based technologies in military applications start? To find the answer to this question, we must go back to the cold war era. During the cold war, the United States military and its allies were

expecting to fight out numbered in conventional weapon systems. To prevail on a battlefield in that environment, it was necessary to develop the ability to give our forces a significant edge in combat efficiency and effectiveness. Technology over the last two decades provided the answers. The power of the computer gave us tremendous improvements in electronic intelligence gathering capability and dissemination, precision guided munitions, stealth technology and communications to name a few of the more important innovations. Improvements in intelligence capability translated into the ability to identify and acquire targets rapidly and at longer ranges.

Precision munitions provided the ability to kill targets at a significant standoff distance and begin attriting enemy forces before they could be committed to the decisive battle with friendly forces. Stealth technology provided friendly aircraft the ability to penetrate enemy defenses undetected and destroy command and control systems, air defenses, and engage/destroy follow on echelons well before they could be in place to influence the battle. Improved communications coupled with the other advances, particularly in intelligence gathering, gave the U.S. Armed Forces the ability to provide the commander better situational awareness and the ability to act quicker and more decisively to offset the numerical advantages of the Cold War foes.

The first opportunity to test these new capabilities came with the war against Iraq. Secretary of Defense William Perry put it best in a 1991 Foreign

Affairs article. "Much of the U. S. military technology displayed so dramatically in Desert Storm had been conceived and developed to offset Soviet numerical superiority in conventional weaponry. The goal then had been to find ways of giving American tanks and other items of major weapons systems a competitive edge with things that would multiply their combat effectiveness. These "offsetting" supplements emerged from modern electronics and computers that promised better intelligence, more effective command and control, and more precision weapons guidance."[3]

What distinguished the American operations in Desert Storm from previous conflicts were new systems and a refined approach to warfare, Defense Secretary Perry argued. "Intelligence sensors, precision navigation data, and communications gave the coalition field commanders an understanding of the battlefield never achieved in previous operations. The ability to suppress the opponent's defenses was unprecedented as well, and precision-guided weapons provided dramatic battle leverage. But as impressive as each of these capabilities were by themselves, their effectiveness when combined was the most telling: All of these were links in the chain of effectiveness, and if any one had been removed, the overall effectiveness of the chain would have been diminished."[4]

Defense Secretary Perry coined the phrase "system of systems" to describe the integration desired to link the weapon systems for maximum effectiveness

as well as better techniques for fighting. The expectation of the "system of systems" is to harness the full potential for existing and programmed weapons platforms through the use of existing and emerging information technologies. The concept incorporates the input from the Combatant Commanders (Commander in Chief {CINC} of Unified Commands) who must fight the weapon systems and forces jointly.

DEFINING THE SYSTEM OF SYSTEMS

What is the "system of systems"? When broken down into components, the phrase has two parts with different meanings. The first part of "system of systems" refers to integrating technologies, doctrine, and techniques employed to gain the maximum benefit of the military forces and weapons. The latter refers primarily to the military forces (soldiers, sailors, airmen, and marines) and their weapons (tanks, artillery, aircraft, ships, etc). Farther defining the systems part of the "system of systems" first will help to determine what needs to be integrated.

Many of the military weapon systems that make up the system of systems were listed into three categories by Admiral William Owens, former vice chairman of the Joint Chiefs of Staff. Figure 1 contains an acronym listing of the weapons and systems in or entering the U.S. military inventory.

The first category is intelligence, surveillance, and reconnaissance (ISR) systems. The systems included in this category are sensors and sensor

platforms that provide the means and ability to electronically collect information on and above a wide geographical area. They give commanders a view of where enemy forces are and what they are doing as well as the ability to keep track of friendly forces. In other words, they provide a significantly enhanced view of the battlespace in real or near real time and in all weather conditions, day or night.[5]

Weapons and Systems in or entering U.S. Military Inventory

ISR	C41	PRECISION FORCE
AWACS	GCCS	SFW
RIVET JOINT	MILSTAR	JSOW
EP-3E	JSIPS	TLAM (BLK III)
JSTARS	DISN	ATACMS/BAT
HASA	JUDI	SLAW
SBIR	C4I FTW	CALCM
Tier 2+	TADIL J	HAVE NAP
Tier 3-	TRAP	AGM-130
TARPS	TACSAT	HARM
MTI	JWICS	AIR HAWK
REMORS	MIDS	SADARM
MAGIC LANTERN	SONET	HELLFIRE II
ISAR	LINK-16	TLAM (BLK IV)
FDS	DMS	JAVELIN
ATARS	SABER	THAAD

Figure 1

The second category is command, control, communications, computers and intelligence (C4I) systems. "Advanced C4I are the technologies and techniques used to translate the enhance battlespace awareness of what is occurring in a broad geographical area into an understanding of what is taking place there, and communicate that understanding quickly, surely, and

accurately--in usable form--to combat forces. It is where processes like target identification, mission assignments and force allocation take place. It is the realm in which we convert the understanding of a battlespace to missions and assignments designed to alter, control, and dominate that battlespace."[6]

The final category is precision force. "Many understand this category to be precision guided munitions, but it includes much more. It is a broader concept that emphasizes speed, accuracy, and precision in the use of force and therefore encompasses all our forces, the infantry as well as strategic bombers, and includes things like information warfare."[7]

In my opinion, a fourth category should be added. Perhaps an appropriate name for this fourth category would be Advanced Battlespace Information Systems (ABIS) after the study commissioned by Dr. Anita Jones, Director of Defense Research and Engineering. "ABIS is defined as a federation of systems that form the underlying grid of flexible, shared, and assured information services and provides advanced capabilities in support of new command and control and force employment concepts."[8] It would incorporate the fields of new research required to integrate the existing systems discussed above to meet the requirements of the CINCs who must employ them. This fourth category takes us more into the realm of new and emerging information technologies such as networked information systems.

That technology, with open systems architecture, was a way to achieve systems integration and provide large volumes of data whenever and wherever it was needed providing an operational and strategic advantage. The sensors see the battlefield, C4I systems transmit that information to the commanders in a real or near real time that they might mass precision force to kill those targets while minimizing risk and exposure of friendly forces. Networking gave the ability for many to see all the information at the same time or only that portion of the information required for them to act. More importantly, networking gave CINCs an enhanced ability to fight forces jointly.

BRINGING IT ALL TOGETHER

Many of the weapon systems discussed earlier that are currently in or entering the U.S. Armed Forces inventory are the product of independent service initiatives. The norm for weapons' procurement at the time was service autonomy and separation. Although some very capable weapon systems evolved, there was very little interoperability between unique service requirements. Urgently needed to harass their full potential was a means of unifying the divergent weapons systems for joint warfighting. Two capstone events provided the catalyst.

The first was the Defense Reorganization Act of 1986, commonly referred to as the Goldwater-Nichols Act. The Goldwater-Nichols Act provided an emphasis on jointness. It defined the roles of and gave specific powers to the

Chairman of the Joint Chiefs of Staff, the Joint Staff, the CINCs and the individual services. Specifically, as a result of Goldwater-Nichols, individual service role are to recruit, train, equip and provide forces to the CINCs, who plan and deploy those forces in support of theater-wide joint operations. Goldwater-Nichols also provided a mechanism for the CINCs to influence service procurement requirements and add an integrated or joint flavor.[9]

The second catalyst was appointment of Admiral William Owens as Vice Chairman of the Joint Chiefs of Staff. Building on the initiatives established by Defense Secretary Perry, Admiral Owens became the champion of the information technology cause. Recognizing how potent the individually fielded systems were and the potential of those systems scheduled to be fielded between now and 2003, he sought to ensure that future expenditures of scarce defense dollars were appropriately prioritized to achieve what he called a qualitatively new order of military power.

Admiral Owens, with the support of General John Shalikashvili, Chairman of the Joint Chiefs of Staff, influenced the prioritization process first through the Joint Requirements Oversight Council (JROC) which he chaired. "The JROC allows the military leadership to screen acquisition proposals. Admiral Owens focused the JROC on the kind of systems integration that lay at the heart of his argument, and fed the resulting recommendations into the

mainstream of the Department of Defense Planning, Programming and Budgeting System."[10]

The primary vehicles used to ensure the new set of priorities were given due consideration were the Chairman's Program Assessment and the Chairman's Program Recommendation. "These documents are also a product of the Defense Reorganization Act of 1986 which requires that the Chairman of the Joint Chiefs of Staff provide the Secretary of Defense with a separate assessment of the military service programs and alternative recommendations on resource allocation."[11] Admiral Owens, in championing the cause of information technology, focused limited defense spending on integrating what had been separate, individual Service programs. This was the first giant step toward true jointness as well as the first real attempt to force the services to focus on integrating combat capabilities.

Another important aspect of shifting to information technologies has to do with costs and the shrinking defense budget. Dual use and/or commercial off the shelf technological innovations adapted to military use are cheaper than researching and developing capabilities specifically for military use. They are also saving a significant amount of time between identifying a capability and getting the product in the field especially solutions for joint warfare.

ARE WE HEADED IN THE RIGHT DIRECTION?

The best way to answer this question is to view information technologies from the end, ways and means paradigm. The end or ultimate goal is to achieve dominate battlespace knowledge as defined in the introduction section of this paper as well as gain the ability to more quickly tailor and deploy a force. The ways to achieve that end is through the focused application and use of existing and emerging information technologies coupled with doctrinal changes in how to fight. The means to achieve the desired end is by adapting existing technology to maximize the potential of weapons platforms and refined deployment options.

From a strategic perspective shifting to information technologies draws on one of the strengths of this nation similar to the way we drew on the industrial strength and capacity of the nation in both world wars. The United States is the preeminent nation in the world in it reliance on information. Information and the ability to make it available when and where needed impacts everything in our society. Information technologies that transport all manner of data and video from shopping at home to interactive video games proliferate through the United States. For the United States military to take advantage of this capability can be seen as a natural flow of events.

From the U.S. Army's standpoint, Force XXI is the interim shift to make advantageous use of available technologies. It is an interim step because it

represents a product improved force. Force XXI boasts 72 new innovations. At the core design is a computer "appliqué" system which refers to a tactical internet that enhances a commanders situational awareness. On a computer screen, commanders can see the location of forces in the field, artillery postures, aviation and air defense activity, intelligence estimates, supply levels and weather reports.[12] In other words, everything of military significance on the battlefield. This makes the tactical internet not much different from the internet we access daily from our homes or offices. Hence, the capacity exists to easily get more information than is needed to do ones job. The key is to get the right information to the right place and at the right time so that it can be put to good use; the very idea and intent of Dominant Battlespace Knowledge.

So the clear answer to the question, are we headed in the right direction, is unequivocally yes as long as the end, ways, and means remain constant. Should the ends change to utilization of technology to reduce manpower, then the answer would have to be maybe. There are clearly some efficiencies to be gained from technology like maybe reduce the size of a crew by one or two personnel but to use it to reduce an Army Division from 18,000 to 15,000 personnel cannot be determined without adequate testing of the combat capabilities of the downsized organization.[13] To do otherwise will bring to the forefront an additional debate; that of a hollow service.

The size of the Armed Forces should be derived from the National Security Strategy looking at the interests of the Nation and the threats to those interests. The Armed Services and the security of the Nation are both put at great risk if the military is sized by any means other than a valid consideration of defense against threats to National interests.

VULNERABILITIES

What makes the Armed Service and the Department of Defense vulnerable by utilizing information technologies? To clearly understand the vulnerability of Defense systems, it will be helpful to understand how and why information flows as it does within the Defense Department.

As a result of drawdowns and consolidations over the last few years, the vast majority of the Armed Forces are stationed in the continental United States (CONUS) with an increasingly smaller number of them maintaining a forward deployed presence. Strategically, to respond to worldwide contingencies, forces deploy from CONUS maintaining a support tail linked through the supported CINC and service component to the national industrial base. These links are generally networked over a communications infrastructure that make up both the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII), since 95 percent of the military's communications travel over the NII.

"Currently, the Defense Department offer a vast information infrastructure target of computers and networks that must be protected. This infrastructure includes more than 2.1 million computers, 10,000 local area networks, 100 long distant networks, 200 command centers and 16 central computer processing centers, or megacenters. More than 2 million defense computer users and an additional 2 million nondefense users do business with the defense department."[14] "These defense systems contain very valuable and sensitive information, including commercial transactions, payrolls, sensitive research data, intelligence, operational plans, procurement-sensitive source selection data, health records, personnel records and inventory and asset visibility. They make attractive targets for individuals or organizations that are seeking monetary gain or that are dedicated to damaging the Defense Department and its operations."[15]

"The Department of Defense computers were attacked an estimated 250,000 times in a single year, with most of the attacks going undetected."[16] "Under the Defense Information Systems Agency's (DISA) vulnerability analysis and assessment program, experts attempted to penetrate computer systems at various military and defense agency facilities via the internet. Since the program's inception in 1992, the agency has conducted 38,000 attacks on defense computer systems to test their protection mechanism. Successful access was gained 65 percent of the time. Of the successful attacks, only 988-

approximately 4 percent-were detected by the targeted organizations. Of the attacks detected, only 267, or roughly 27 percent, were reported. Only one in 150 successful attacks drew an active response from those organizations involved."[17] This is a clear indication of how vulnerable the Armed Services and the Department of Defense are to attack.

Here is one outside example of an attacks shows the strategic implications of the vulnerability. Dutch computer hackers penetrated U.S. military networks, stole secrets during the Persian Gulf War and offered them to Iraq. The secrets could have altered the course of the war, but the Iraqis allegedly never used the information, fearing a hoax. The hackers, using the internet, allegedly pilfered information from 34 U.S. military sites.[18]

The NII is itself highly vulnerable and because of the Defense Department's increasing dependency on it, it is becoming more and more essential to everything the military does with information. The total vulnerability of the NII is difficult to gauge because data is available only on a very small portion of it. Commercial companies are hesitant to report break-ins for fear of loss of public trust especially banking institutions. Testifying before a hearing of a Senate Governmental Affairs subcommittee on June 25, 1996 , Central Intelligence Agency (CIA) Director, John M. Deutch warned that the country is likely to experience some very large and uncomfortable destruction of vital computer systems at the hands of foreign terrorists or

hostile nations in coming years.[19] "According to a survey conducted by WarRoom Research, almost half of 200 large US companies had their computers broken into over the past twelve months and several had steep losses as a result. Among companies that reported intrusions and could assess damages, 84 percent put their losses for each successful attempt at $50,000 or more."[20]

Additionally, some commercial off the shelf (COTS) technology leave us vulnerable to a wide variety of cyberbombs.[21] Few of these products are what can be defined as "trusted" meaning that there are no procedures to verify or certify that the products are free of bugs, back doors or just plan mistakes before they are introduced into existing networks. "A team of Princeton University researchers say they discovered the most serious security flaw yet in the widely used Java programming language from Sun Microsystems Inc. The team said the flaw could make it possible for unscrupulous hackers to destroy files or cause other types of damage on any personal computer that uses Netscape Communications Corp's Navigator program."[22] Netscape's Navigator program is the most commonly used World Wide Web (WWW) surfing software in the Defense Department.

Of course, steps are taken to correct these deficiencies once they are identified and software updates are provided by the manufacturer, usually free of charge. But not everyone gets the update so it seems. "The head of the

Computer Emergency Response Team (CERT) once estimated that well over 90 percent of all reported break-ins were made possible because hackers could exploit known but uncorrected weaknesses of the target system. For instance, the method hackers used to get into Rome Laboratory's computers in 1994 and Los Alamos' computer in 1996 was an unfixed bug in the UNIX sendmail program that was used for the infamous internet Worm incident in 1988. Fewer than one incident in ten came under the category of no-one-knew-that-could-be-done, but most of these were understood to be theoretically possible, even if the exact method used was not."[23] To make matters even worst, the Federal Bureau of Investigation Bulletin stated that by the year 2000, almost 90 percent of all criminals will be computer literate.[24]

Tools used by hackers are readily available on the Internet. "Informal hacker groups, such as the 2600 Club, the Legion of Doom and the Phrackers Inc., openly share information on the Internet about how to break into computer systems. This public forum, when combined with the availability of user friendly and powerful attack tool, makes it easy for anyone to learn how to attack systems and to refine attack techniques."[25] If this does not make it imperative that actions be taken immediately to protect against unwanted intrusions, then consider that "sixty percent of all Ph.D.s in computer security by American universities went to citizens of Islamic or Hindu countries."[26]

All of this illustrates that there is indeed growing vulnerability to information systems. Because the vulnerability can effect almost every aspect of the Nation, including vital services and institutions, its security is a growing National Security concern. The Department of Defense has a prominent role to play for self protection purposes as well as for the good of the Nation.

PROTECTING OURSELVES

One of the first steps in defending against the threats posed to the NII is awareness. Awareness fosters debate and concern which leads to actions. Over the last few years there has been a growing public awareness of the vulnerability of the NII and as a consequence of its vulnerability, there is an increasing awareness of the threats posed to the Defense Department and other government agencies.

The greatest indication of awareness at the national level is Executive Order 13010, published July 15, 1996, which established the President's Commission on Critical Infrastructure Protection . It states that "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government. Threats to these critical infrastructures fall into

two categories: physical threats to tangible property; and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures. Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."[27] Their task is to bring together the combined forces of the government and private sector to advise and assist the President of the United States by developing a strategy for protecting and assuring the continued operation of this nation's critical infrastructures. The commission has a year to publish a report. If done correctly, their report should have far-reaching consequences; though change is not likely to happen very rapidly. Areas where influence is expected most from the report are:

> Laws - this area always lags behind in times of rapid change. Though some progress has already been made in this area domestically, FBI director, Louis Freeh, in a speech to the International Computer Crime Conference on 11 March 1997, said "the FBI needs worldwide cooperation among law enforcement agencies to catch bandits in cyberspace--a new frontier where international borders do not exist."[28] Individual privacy versus the need to track, capture and convict crinimal is vital to establishing appropriate laws for protecting the NII and other information infrastructures.
>
> Funding - could be in the area of tax incentives for private industry to take appropriate steps, grants for farther research and development and direction to government agencies to pull together and focus spending in critical areas.
>
> Ciritcal Infrasturcture - identify what is truly critical and what the absolute minimum essential infrastructure requirement is, since

everything obviously can't be protected.

In April 1995, CIA Director John Deutsch (then deputy secretary of defense) said at his Senate confirmation hearing, "Protection of the NII is an important subject...which we don't have a crisp answer to. Understanding that we have a vulnerability, and knowing what to do about it... are two different things."[29] A little more than a year later, the CIA announced plans to create a "cyberwar" center at the National Security Agency to protect the bits and bytes that weave the nation together.[30]

The Department of Defense has made some significant advances in efforts to protect against vulnerabilities. Similar to the President's Commission on Critical Infrastructure Protection, the Defense Department commissioned a study by the Defense Science Board which made 13 specific recommendations. "Among those recommendation was the establishment of an "information-warfare" czar and an "information-warfare" center in the within the U.S. intelligence agencies."[31] These two recommendations have already been enacted with Assistant Secretary of Defense for Command, Control, Communications and Intelligence appointed as the central DOD point of contact and the National Security Agency's establishment of its 1000 man "cyberwar" center.

Another recommendation of the study was for DOD to spend $580 million in coming years on research and development, mainly in the private sector, to

develop new hardware and software to provide security such as a system for automatically tracking hacker attacks back to their origins.[32] Two recommendations not likely to be adopted are to give the Defense Department legal authority to repel and pursue those who try to hack into its computer systems, and to eventually disconnect the Defense Department from outside information systems.[33]

The Defense Information Systems Agency established the Global Operations and Security Center which consolidates the functions of its Global (Information Systems) Control Center and the Automated Systems Security Incident Support Team (ASSIST) into a single organization which is structured to detect and react to disruptions in the information infrastructure. Center analysts will use data collected during incidents and intrusions to establish patterns of activity. These patterns are to develop strategic indications and warnings.[34] The Global Operations and Security Center will work hand and hand with the National Security Agency's "cyberwar" center.

The military services have all established information warfare program offices with efforts in defensive systems. The Army, in particular, has made tremendous strides in assuring information security. At Department of the Army level, "the Deputy Chief of Staff for Operations, the Deputy Chief of Staff for Intelligence and the Director for Command, Control, Communications and Computers forms a triad to oversee a Command and Control Protect Program

that is designed to maintain confidentiality and integrity and to make available the information necessary for decision making and control of forces and systems."[35] The Army's focus is on institutionalizing Command and Control protection through education, training and requirements determination following doctrine on Information Operations captured in Field Manual 100-6, Information Operations. The Army will seek to determine realistic vulnerabilities of its systems to attack by using offensive information technology that potential adversaries are believe to possess.[36] The focus of these efforts will be at fixed and tactical facilities.

Although tremendous efforts are being taken at the strategic level of the Army and the other services as a whole, a great deal remains to be done. Continued emphasis on initial and sustainment training of network managers and system administrators is warranted at every level to prevent a recurrence of situations like the one where hackers penetrated 34 sites to gain information on Desert Storm's operations. Making maximum utilization of existing technologies, software or hardware, to protect systems at each level is warranted.

CONCLUSION

Since the time of the cold war, the United States Armed Services has looked to technology to provide a warfighting edge. Over the last decade, a significant number of innovations have materialized to provide that edge and

the future indeed looks bright specifically with the advances made in silicon based information technologies. The armed services have made a conscience choice to continue taking advantage of these technologies in light of the great potential they offer in spite of a growing awareness of the vulnerability they present. The question seems to be "do the advantages out weigh the vulnerabilities?"

The answer is yes, based on the pace at which efforts are on going to harness and use information technology. We've already seen the advantage technology gave us in Desert Shield and Desert Storm and witnessed the enhancements in Bosnia. There is a growing sense of jointness in operations.

Commanders now have better situational awareness than at anytime in history. But we cannot loose sight of the potential vulnerabilities. Significant strides are being made throughout the Department of Defense and the armed services to combat identified weaknesses. At the National level, the President established a Commission on Critical Infrastructure Protection to bring together government and private industry to work collectively to solve the problems. It is now only a matter of time until the vulnerabilities are fixed.

In the interim, prudence dictates moving forward at a measured pace without loosing sight of the objective. From a military perspective that means testing and selecting those innovations that contribute the most to warfighting capability based on a clear vision, adjusting doctrine to take advantage of the

added or new capabilities, and training the force to employ those capabilities to best support the CINCs theater campaign plans.

With the volatile, uncertain, complex and ambiguous environment that exists in military operations, technology provides a means to make the "fog of war" less opaque. A great start has been made. The future will be what we make of it.

ENDNOTES

[1]United States Senator John McCain, "Reday Tomorrow: Defending American Interests in the 21st Century," March 1996.

[2]William Owens, "Dominant Battlespace Knowledge: The Emerging U.S. System of Systems," undated, <http://www.ndu.edu/ndu/inss/books/dbk/dbkch01.html>, 11 October 1996.

[3]William J. Perry, "Desert Storm and Deterrence," Foreign Affairs 70 (Fall 1991): 66.

[4]Ibib, 76-77.

[5]Owens, 1-2.

[6]Ibib.

[7]Ibib.

[8]Robert K. Ackerman, "Battlespace System Offers Data Anywhere, Anytime," Signal 51, no. 5 (January 1997): 26.

[9] John P. White, "Defense Organization Today," Joint Force Quarterly 13 (Autumn 1996): 19.

[10]James R. Blaker, "Understanding The Revolution in Military Affairs: A Guide to America's 21st Century Defense," Progressive Policy Institute, no. 3 (January 1997): 3.

[11]Ibib .

[12]Bradley Graham, "Army Trying Out Electrons to See If It Can Get Small and Faster 2-Week Dry Run in the Mojave Desert Ends in Something of a Draw," Washington Post, 31 March 1997, sec. A, p. 4.

[13]Ibib.

[14]Clarence A. Robinson, Jr., "Western Infrastructures Face Rogue Data Stream Onslaught," Signal 51, no. 5 (January 1997): 35.

[15]Ibib.

[16]Gary H. Anthes, "U.S. easy target for cyberattacks," Computerworld 30, no. 22 (1996): 7.

[17]Robinson, 32.

[18]Douglas W. Washington, "Onward Cyber Soldiers." Time Magazine 46, no. 8 (1995): 44.

[19]Tim Weiner, "Head of CIA Plans Center To Protect Federal Computers," New York Times, 26 June 1996, sec. B, p. 7.

[20]Quentin Hardy, "Firms are hurt by break-ins at computers," Wall Street Journal, 21 November 1996, sec. B, p.4.

[21]Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," The Washington Post, 16 July 1995.

[22]Don Clark, "Researchers find big security flaw in Java language," Wall Street Journal, 26 March 1996, sec. B, p. 4.

[23]Martin C. Libicki, "Defending the National Information Infrastructure," undated, <http://www.ndu.edu/ndu/inss/actpubs /niitemp.html>, 11 October 1996.

[24]Richard S. Groover, "Overcoming obstacles: Preparing for computer-related crime," FBI Law Enforcement Bulletin 65, no, 8 (1996): 8.

[25]Robinson, 33.

[26]Libicki.

[27]Executive Order 13010, "President's Commission on Critical Infrastructure," 15 July 1996, <http://jya.com/eo13010.text>, 12 March 1997.

[28]FBI Director Louis Freeh, speaks to the International Computer Crime Conference, 11 March 1997, New York.

[29]Munro.

[30]Weiner.

[31] Thomas E. Ricks, "Information-Warfare Defense Is Urged: Pentagon Panel Warn of Electronic Pearl Harbor," Wall Street Journal, 6 January 1997, sec. B, p. 2.

[32]Ibib.

[33]Ibib.

[34]Robinson, 31.

[35]Clarence A. Robinson, Jr., "Army Information Operations Protect Command and Control," Signal Special Edition (Undated): 14.

[36]Ibib.

BIBLIOGRAPHY

Ackerman, Robert K. "Battlespace System Offers Data Anywhere, Anytime." Signal 51, no. 5 (January 1997): 26-29.

Anthes, Gary H. "US easy target for cyberattacks." Computerworld 30, no. 22 (1996): 7.

Blaker, James R. "Understanding The Revolution in Military Affairs: A Guide to America's 21st Century Defense." Progressive Policy Institute, no. 3 (January 1997): 3-12.

Clark, Don. "Researchers find big security flaw in Java language." Wall Street Journal, 26 March 1996, sec. B, p. 4.

Executive Order 13010. "President's Commission on Critical Infrastructure." 15 July 1996. <http://jya.com/eo13010.text>. 12 March 1997.

Freeh, Louis, FBI director. Speaks to the International Computer Crime Conference, 11 March 1997, New York.

Graham, Bradley. "Army Trying Out Electrons to See If It Can Get Small and Faster 2-Week Dry Run in the Mojave Desert Ends in Something of a Draw." Washington Post, 31 March 1997, sec. A, p. 4.

Groover, Richard S. "Overcoming obstacles: Preparing for computer-related crime." FBI Law Enforcement Bulletin 65, no. 8 (1996): 8-10.

Libicki, Martin C. "Defending the National Information Infrastructure." undated, <http://www.ndu.edu/ndu/inss/actpubs /niitemp.html>. 11 October 1996.

McCain, John, United States Senator. "Ready Tomorrow: Defending American Interests in the 21st Century." March 1996.

Munro, Neil. "The Pentagon's New Nightmare: A Electronic Pearl Harbor." Washington Post, 16 July 1995, sec. C, p. 3.

Owens, William. "Dominant Battlespace Knowledge: The Emerging U.S. System of Systems." undated. <http://www.ndu.edu/ndu/inss/books/dbk/dbkch01.html>. 11 October 1996.

Perry, William J. "Desert Storm and Deterrence." Foreign Affairs 70 (Fall 1991): 66-82.

Robinson, Clarence A., Jr. "Army Information Operations Protect Command and Control." Signal Special Edition (Undated): 14-16.

Robinson, Clarence A., Jr. "Western Infrastructures Face Rogue Data Stream Onslaught." Signal 51, no. 5 (January 1997): 31-35.

Ricks, Thomas E. "Information-Warfare Defense Is Urged: Pentagon Panel Warn of Electronic Pearl Harbor." Wall Street Journal, 6 January 1997, sec. B, p. 2.

Washington, Douglas W. "Onward Cyber Soldiers." Time Magazine 46, no. 8 (1995): 37-44.

Weiner, Tim. "Head of CIA Plans Center To Protect Federal Computers." New York Times, 26 June 1996, sec. B, p. 7.

White, John P. "Defense Organization Today." Joint Force Quarterly 13 (Autumn 1996): 18-22.