Information Operations: The Command and Control Warfare (C2W)

CSC 1997

Subject Area - Electronic Warfare (EW)

EXECUTIVE SUMMARY

SUBJECT: Information Operations: The Command and Control Warfare (C2W)

AUTHOR: Major Steve High, USA

DISCUSSION: The Informant Age and the increased use of information-based communications systems has created incredible possibilities and vulnerabilities for the users of such systems. These technological opportunities and vulnerabilities are extremely apparent in command and control warfare, a subdivision of information warfare, a branch of information operations. The U.S. Army provides examples of the continuing search by the military community to understand fully and employ effectively the tools of information operations for continued success in identifying and neutralizing future threats.

THESIS: In the Information Age with such tremendous advances in information technology, we are exceeding levels of communication never experienced before. What is of particular importance to the military are the advanced information communication networks which create information infrastructures for global information infrastructures (GII), national information infrastructures (NII), and of concern to the military, the defense information infrastructure (DII). These interconnected systems permit the rapid exchange of information and ideas throughout the world and an interdependence among the users. This interdependence further produces a dangerous dichotomy of use. At the same time that these technological advances provide users new and exciting capabilities and opportunities to transmit information, they also expose the users of these systems to incredible vulnerabilities. For the Department of Defense (DoD), a user of the information infrastructures, this dichotomy is a lethal two-edge sword. On one side, a user may employ offensive information operations to attack the command and control elements of an adversary, while on the other side, the adversary may attack first or have highly developed defensive measures. All of the DoD Service components are developing technology and systems to increase the lethality these information technology advances in offensive information operations, while at the same time they strive to diminish lethality of potential adversaries through protective defensive information operations. This paper will focus upon the U.S. Army's response to the dichotomy of use in information operations with respect to command and control warfare (C2W).

CONCLUSION: Understanding the capabilities as well as the vulnerabilities associated with the computer-based information systems is essential in order to achieve and maintain information superiority.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **1997**	2. REPORT TYPE	3. DATES COVERED **00-00-1997 to 00-00-1997**

4. TITLE AND SUBTITLE
Information Operations: The Command and Control Warfare (C2W)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
United States Marine Corps,Command and Staff College, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068

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
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**17**	

INFORMATION OPERATIONS:
COMMAND AND CONTROL WARFARE (C2W)

> Our intelligence agencies have acknowledged that potential adversaries throughout the world are developing a body of knowledge about the Defense Department and other government computer networks. According to these DoD officials, these potential adversaries are developing attack methods that include sophisticated computer viruses and automated attack routines [that] allow them to launch untraceable attacks from anywhere in the world. Our government understands that many countries are developing offensive information-warfare capabilities. . . At some point, we must consider how we would respond to an actual attack if one were to happen . . . . I'm not speaking of military force, but I'm speaking of perhaps using some of the tools of information warfare to basically back up on a system that carries out the attack, so that the information system itself is the subject of very several punishment and counterattack, wherever it's coming from . . . If we don't think in that vein, then we're just basically going to be in the game-playing where everybody tries to hit us and it becomes a game as to how we can defend against it. it seems to me we've got to leap into the thought process . . . of trying to use information warfare itself to be able to make an attack or even a serious illegal probe very unattractive to the potential perpetrator.[1]

I. Introduction

Information Age technology is profoundly altering the nature of warfare as we enter the 21st Century. This point was highlighted when former Secretary of Defense William Perry asserted that "We live in an age that is driven by information. Technological breakthroughs . . . are changing the face of war and how we prepare for war."[2] The dynamics of the Information Age are creating unique challenges for Information Age warfighters. How the United States, and particularly the Department of Defense (DoD), respond to these challenges will have a tremendous bearing on our nation's security.

The information environment in which the global community operates, is transforming everyday life, industrial and financial markets, and even how governments relate with each other. Today, with the unprecedented advancements in information technology, communication capabilities based upon these information-based systems have reached levels never experienced before. The military no longer operates in a completely isolated information environment. The various communication infrastructures which comprise today's information environment are extremely interdependent.

The global information environment (GIE) is the information environment in which all organizations, individuals, or systems, “most of which are outside the control of the National Command Authorities,” collect, process, and disseminate information to national and international audiences.[3] All military operations occur with the GIE, which is “both interactive and pervasive in its presence and influence,” and permit aspects of such military operations to be made known to the global audience in near-real time and without the benefit of filters.[4] The Global Information Infrastructure (GII) is the worldwide interconnection of communications networks, computers, databases, and consumer electronics which make vase amounts of information available to users. It includes a wide range of equipment,[5] physical facilities used to store, process, and display information; and the personnel who handle the transmitted information.[6] The National Information Infrastructure (NII) is similar in nature to the GII, however, it relates only to the national information environment.[7]

Of primary concern to DoD is the Defense information Infrastructure (DII). This infrastructure is composed of shared interconnected computer systems, communications, security, data appellations, people, training, and other support structures serving DoD’s local, nation, and worldwide information needs.[8] This systems carries DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. On the one hand, the labels used to identify these information systems may be misleading as there are no “fixed boundaries in the information environment,” and, on the other hand, the nature of the open and interconnected systems is generating rapidly expanding GIIs which enfolds the NII, and DII, which is deeply embedded and integrated within the NII.

Thus, the United States' dependence on information and information systems is a sharp, dual edge sword. On one side are the tremendous opportunities and capabilities which stem from the incredible advances in communications technology, while on the other side, are the vulnerabilities which expose the user to a complete range of threats -- computer hackers, criminals, vandals, terrorists, and even nation states. "National security in the Information Age poses significant challenges for the Department of Defense and the nation. All organizations and decision-makers, while embracing the advantages offered by information-based technologies, must respond to the significant vulnerabilities inherent in the systems upon which their capabilities depend."[9]

The Department of Defense and all of its Service components have been and are continuing to develop technology and systems to increase the lethality of information-based systems technology in offensive information operations, while at the same time striving to diminish the capability of any potential adversaries through protective defensive information operations. Section II of this paper will provide a brief overview of information operations and the nature of the dichotomy of dual purpose regarding the use of information infrastructures. Section III will focus upon the Department of the Army's response to the dichotomy of use in information operations with respect to command and control warfare (C2W).

II. Information Operations - An Overview

The dichotomy of use of information-based systems is a fundamental aspect of what is now known as "information operations."[10] Although the term information warfare developed nearly twenty years ago,[11] use of information-based technology systems during the Gulf War prompted DoD to dramatically increase research and development in this area.[12] DoD is continuing to harness the full scope of the capabilities and vulnerabilities of information-based technologies and systems. Gathering, exploiting, and protecting information have been critical elements in command, control, and intelligence throughout history.   In the future, the importance of information will not change. "What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology. While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact."[13]

Information operations apply across the spectrum of military operations and at every level of warfare. Information operations may be employed to achieve national objectives without resorting to force or to act as a force multiplier in the event force is required. For DoD, the ultimate strategic goal of offensive information operations is to affect a human decision maker to the degree that an adversary will cease actions threatening to US national security interests. At the tactical and operational levels, information operations target and protect information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems.[14]

The concept of information dominance or superiority is the key element for operating effectively within this new environment of interdependent information systems. Information dominance/superiority is the capability "to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[15] To achieve information dominance, the commander "must be able to dominate both the traditional maneuver-oriented battlefield and the *military information environment*," defined as that "portion of the GIE relevant to his operation."[16] To achieve the latter, the commander directs the acquisition, use, and management of friendly and enemy information and conducts command and control warfare (C2W) attack and protect operations.

Information operations conducted during periods of conflict or war are called information warfare operations.[17] Information warfare can be waged in wartime "within and beyond the traditional military battlefield."[18] As a subset of information warfare, command and control warfare (C2W) is an application of information warfare in military operations that specifically attacks and defends the command and control (C2) target set.[19] It should be noted that the capabilities and disciplines employed in C2W such as psychological operations (PSYOP), deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, can be employed to achieve effects outside of the C2 target set.[20]

The threat in the information age is unique. The systems and capabilities of the information age are evolving at blinding speed, with computer power doubling every eighteen months or less, and evermore-powerful hardware becoming available to potential "bad actors" for a low entry cost. It is estimated that over one hundred countries have the technology to attack U.S. commercial and military information systems. Furthermore, there is evidence that at least half of these have attempted to penetrate these systems. Their intrusions range from simply looking around the system, to destroying systems and perpetrating fraud on the telephone and banking institutions. Statistics indicate that an estimated that three hundred people a day attempt to intrude into the Pentagon's computer systems.[21] Due to the speed at which these intrusions occur, it is extremely difficult to know when a system is under attack. Therefore, there may never be an opportunity to identify the intruder. Also it is difficult to determine the extent of the havoc wreaked on compromised systems because there is no bomb damage assessment capability for information systems.

The enemy can be any person, group, or nation. The enemy can come from anywhere. The enemy may be from within a country or organization. Among the potential targets of terrorist groups or enemy states might be the nation’s power grid, the public telephone switching system, the stock markets, the Federal Reserve, the Internal Revenue Service, “strategic” companies, the research-and-development structure, the air traffic control system, and the national banking system. Some have asked the question “What if Saddam Hussein, prior to his invasion of Kuwait, had hired 20 hackers to disrupt the American economy?" He would have drastically changed how the United States would have responded if he possessed the right capability to shut down the phone system by crippling AT&T’s network, and destroying the financial network.

For private industry, the vulnerabilities of the information age forge a new relationship between human resources officers and network managers - “the network managers want a heads-up that someone is about to be fired so they can immunize the local area network from revenge.”[22] The former director of the National Security Agency, Vice Adm. John M. McConnell, USN, (Ret.), conducted experiments to see the vulnerability of the nation’s supposedly “secure” computer systems. He concluded that some could be cracked “with $10,000 worth of equipment, a half-dozen college students, some pizzas, and beer.”[23] “While the scope of the problem largely is speculative, hacker attacks cost U.S. business between $100 billion and $100 billion each year,” said Dr. Fred Giessler, professor of information warfare at NDU. This is of definite concern to the government because “[f]raud on this scale constitutes a threat to national security.”[24]

Despite the fact the that current Internet system is a result of the internet system DoD developed in the late 1960’s linking research laboratories, universities, and the Pentagon, there are indications that DoD is concerned with the growing popularity of computer networks such as the Internet, makes defense data and systems more vulnerable. The Internet computer network links more than 160 countries and has hundreds of millions of users. It carries financial and military information systems, for example, as well as personal communications. As a result, the Pentagon is proposing to spend $700 million in research and development funds through 2001 to develop encryption techniques and other information infrastructure protection devices.[25] Because of the Internet's size, an attack could come from anywhere. The problem for the Defense Department is that in order to share information, Pentagon systems must be linked to the commercial information infrastructure through the commercial phone system and Internet.

The threat situation is difficult to address because the nature of the threat has not been determined fully. There is a great difficulty in dealing with a threat when you do not what it is. For DoD this is a critical point in dealing with command and control warfare. The information-based systems which provide DoD with incredible capabilities to strike at the C2W elements of an adversary are the same ones which may be used against DoD.

III. Command and Control Warfare - The Dichotomy of Use and The Department of the Army in the Information Age

"Any military - like any company or corporation - has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information, while selectively denying or distributing it to its adversaries and or allies."[26] This is the essence of C2W. An integrated military strategy focuses on attacking the command and control capabilities of the enemy while protecting friendly command and control capabilities. Its purpose is to deny critical command information from being passed within the enemy's internal lines of communication and protecting and enhancing friendly command and control capabilities.

C2W is more than an inventory of equipment to strike at the enemy. It is a strategy which applies the equipment or informational advantage with a plan to cut the head off or remove the operating capability from the enemy. The critical capability is not always the same when targeting the enemy's C2 system. The ultimate reason for targeting the C2 systems is to completely neutralize or destroy, the leader, the army, the will of the people, the will of the military, or the ability of the enemy to act effectively with all parts of its decision making and battle executing functions. The decisions on how to render the enemy useless form the basis of the strategy by which military planners decide specific targets when engaging in C2W.

The U.S. armed forces do not have a monopoly on employing C2W. Our enemies and our allies also possess the capabilities to either counter our C2W efforts or engage our C2 system. The commander will ultimately decide on the priority of the C2W effort in the C2W Annex D of the Army OPORD. However, the battle staff will make recommendations based on information received through intelligence sources.

As discussed in Section II above, DoD employs information operations in the full spectrum of military operations. Information warfare is the offensive wartime/conflict time subdivision of information operations, and C2W is a subset of information warfare operations. Within C2W, the military uses operations security, military deception, psychological operations, electronic warfare, and physical destruction as the implementing tools of C2W. These tools have a mutual supporting relationship with intelligence to provide the necessary or time critical information to sever the command and control of the enemy.

A. Capabilities

It should be noted that most of DoD's information operations offensive capabilities for C2W are classified. Additionally, the concept of DoD's "waging war" on the Internet is very disconcerting to the American citizenry. Thus, discussion regarding offensive capabilities is usually very limited. In a discussion on this topic with Richard A. Kaplan, Chief, U.S. Army Land Information Warfare Activity (LIWA), we discussed the classified information nature of most of the capabilities. Nevertheless, it is clear that developing technology plays an important role in the ability of the commander to receive more complete information of the battlespace. Users will benefit from the potential and greater quality decisions due to the rapid increases in technology. Provides the maneuver commander support needed for potential rapid maneuver in terms of both time and space. Finally, an increase in technology will provide an increase in a unit's flexibility and ability.

FM 100-6 presents a section regarding potential future acquisitions. There are several interesting concepts listed in this section:

> Tactical Internet capable of direct communications with all users;
>
> Direct broadcast satellites able to communicate at real time or near real time;

Image compression and transmission technology to allow for transfer or images for video linking and mission execution; and

Multimedia technology to enable three dimensional presentations.

The centerpiece of current technology and future technology is the solider and the leader. If soldiers and leaders are well-trained and able to harness the future technological breakthroughs, they will enhance our C2W capability as much as any digitized and automated information systems. However, when combined appropriately, we will maintain the decisive edge.

B. Vulnerabilities

The threat to the military in the past was usually a known entity. Templates were available to protect the size and composition of the enemy. Today, the ability to protect from or guess what the potential will look like or what weapons they may bring to the battle is a difficult challenge. Past predictions were based usually on the number of tanks, aircraft, artillery tubes, and even nuclear missiles. The current threat has no template. It might not number over one or may range in size to the largest nation on the globe. The current threat and the threat of the future is invisible. The threat could invisibly reside in the electronic arena. This amorphous enemy could be described as passive, remote, readily available, and profitable. The most likely targets are the automation and electronic systems; navigational aids, and global positions devices, communication networks or nodes, space systems, flight controls, data links, and data bases. An invisible and undeniable enemy can strike at our C2 systems with on warning.

This section will explore the following five areas of vulnerability: 1. financial resources; 2. the increased need for training; 3. the need for new equipment; 4. the heavy reliance upon an interdependence of civilian information systems; and, 5. the need to have interservice and interagency compatibility of information systems.

1. Financial Resources

There has been a reduction in funding while at the same time there has been an increased reliance on automated processing and information systems.[27] The Army's FORCE XXI focuses on the digitized battlefield, an upgrade from the current systems will require additional funding to maintain a decisive edge in technology purchase and acquisitions. Funding is essential to maintain future upgrades in software, as other technology. Otherwise, the systems in use will be of no value as such items will be outdated.

2. Increased Need For Training

There currently exists a severe lack of training available for information management systems and information systems managers. The Army is focusing on improving the training area in order to keep up with information technology. As of July 1996, there were over 4,000 local area network managers without formal training to certify knowledge of operating systems.[28] The concern in this area is lack of knowledge of the potential security problems and procedures for the information systems.

3. Need for New Equipment

There is a tremendous need for the procurement of hardware systems that will upgrade the Army's existing communication and computer security equipment. Much of the current equipment in use and in the inventory is obsolete or almost obsolete as various repair parts do not exist.[29] With an increasing ability for eavesdropping and monitoring phone lines, communication and computer security equipment will protect the vulnerable dependency on the commercial communication lines.

4. Interdependence on Commercial Information Communications Systems

Nearly "90% of the Army's information distribution systems is owned and operated by non-DoD agencies. This creates a challenge to availability and reliability of information because the deployed force commander no longer controls circuit available integrity, reconfiguration or reconstitution."[30] This defeats the purpose of having such a highly advance system, because if you cannot control it, it is of no use to you.

5. Need for Interservice and Interagency Compatibility

Information systems integration with other services and government agencies is critical for a functional C2W system. The current communications systems each of the service maintains has incompatibility problems. The integration of common hardware and software will allow systems compatibility. "It is intuitive there are potential vulnerabilities associated with the digitized force, and what we need to do is identify those potential vulnerabilities so we can develop appropriate countermeasures."[31]

C. Department of the Army Responses to the Dichotomy of Use

The Army has responded in an aggressive manner to the problems and opportunities inherent in the use of information-based communications systems. Overall, the Army professes that knowledge of the threat is the key to the best defense. The Army first put forth its concept of information operations in the Training and Doctrine Command (TRADOC) Pamphlet 525-69, 1 Aug 1995. This document describes the importance of information and how to win the information war in military operations now and in the 21st Century.[32] The followed up on this pamphlet with its Field Manual 100-6, Information Operations. This manual addresses the operational context of information operations. It also shows the change from the terminology of information warfare to information operations.

The Army leadership formed a C2 Protect Triad consisting of three Lieutenant Generals on the Army Staff: Director of Information Systems for Command, Control, Communications, and Computers, DISC4; Army Deputy Chief of Staff for Intelligence (DCSINT), and the Army Deputy Chief of Staff for Operations (DCSOPS). The purpose of the Triad is to plan for potential threats and to address all of the protection issues for all levels of command. In order to be able to respond to possible computer intrusions, the Army created its own computer emergency response team (CERT) to investigation and computer problems. DISA performed this function prior to the Army establishing its own capabilities. In order to test the integrity of computer systems, Red Teams have been established to identify and detect vulnerabilities and relay the vulnerabilities to the Service in order to correct the finding. Above all else, the Army created the Land Information Warfare Activity (LIWA) to provide tailored information operations support to land component commanders through technical expertise that does not exist within the general and special staff[33]. "[Battlefield advantages can be gained, if the information operations environment is understood, and especially if a commander knows the information warfare capabilities and how to employ them at the precise time to influence the battle."[34]

IV. Conclusion

The Information Age has bestowed upon the warriors entering the 21st Century challenges never envisioned before. The interdependence of between the military and civilian communications systems poses a challenge for the future cyberwarrior to erase the dichotomy of use inherent in the present information-based communication networks. Understanding the unique relationship between the capabilities and vulnerabilities inherent in these systems is critical for continued successful military operations.

[1] Statement, Senator Sam Nunn (D-Ga.), June 25, 1996, Hearing of the Senate Governmental Affairs Committee, cited in "Cyberstrategic Attacks," Air Force Magazine September 1996: 48.

[2] Peter Constantini, "Technology-Information: Information Warriors Form New Army," Inter Press Service (August 9, 1996).

[3] Dep't of the Army, Field Manual 100-6 (FM 100-6), Information Operations August 1996: 1-2.

[4] FM 100-6, 2.

[5] The GII equipment includes cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, television, monitors, and printers among other items. Joint Pub 3-13, Joint Doctrine for Information Operations, First Draft, 21 January 1997: I-24. This publication is an unclassified document which contains many of the unclassified definitions which are found in the classified DoD Directive (S) 3600.1, Information Operations, (9 Dec 96).

[6] JCS Pub 3-13, I-24.

[7] JCS Pub 3-13, I-25.

[8] JCS Pub 3-13, I-23.

[9] Arthur K. Cebrowski, Vice Admiral, USN, Director for C4 Systems, Joint Staff; Ervin J. Rokke, Lieutenant General, USAF, President, National Defense University, in Memorandum, Subject: Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 4 July 96, in Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, (2nd ed, 4 July 1996).

[10] During the staffing of DoD (S) 3600.1, Information Operations, (9 Dec 96), DoD chose to use the term "information operations" instead of "information warfare" to describe the overall "actions taken to affect adversary information, and information systems, while defending one's own information and information systems." DoD retained the term information warfare but assigned it a much narrower definition: "information operations conducted during time of crisis or conflict to achieve or promote specific-objectives over a specific adversary or adversaries." Joint Pub 3-13, Joint Doctrine for Information Operations, First Draft 21 January 1997: II-17-18, II-20. The definitions in the unclassified Draft Joint Pub 3-13 reflect those unclassified definitions in classified DoD (S) 3600.1.

[11] Dr. Thomas Rona is credited with developing the term information warfare in 1976. He is a preeminent intellectual in the field of information operations. Thomas P. Rona, "Information Warfare: An Age-Old Concept with new Insights," Defense Intelligence Journal, Spring 1996: 53.

[12]Alan D. Campen, ed., The First Information War (Fairfax: AFCEA International Press 1992).

[13]Shalikashvili, General John M., Joint Vision 2010, 1996: 16.

[14]JCS Pub 3-13, I-2.

[15]JCS Pub 3-13, I-19.

[16]FM 100-6, 1-1.

[17]JCS Pub 3-13, 1-20.

[18]JCS Pub 3-13, 1-3.

[19]JCS Pub 3-13, 1-3.

[20]Joint Pub 3-13, I-4.

[21]Stacey Evers, “IW Poses Infinite Questions, Few Answers,” Aerospace Daily June 23, 1995: 472.

[22]Evers, 473.

[23]John A. Tirpak, “The New Role of Information Warfare,” Air Force Magazine, June 1996: 30.

[24]Pat Cooper, "In Cyberspace, U.S. Confronts an Illusive Foe," Defense News, February 1995: 2
.

[25]Cooper, 1.

[26]FM 100-6, 2-8, quoting Alvin & Heidi Toffler, War and Anti-War: Survival At the Dawn of the 21st Century.

[27]Clarence A. Robinson, Jr., “Army Information Operations Protect Command and Control,” July 1996: 49.

[28]Robinson, 48.

[29]Robinson, 48.

[30]Stacey Evers, “Report Points Up Threats to US Army C2 Security,” Jane’s Defense Weekly January 24, 1996: 8.

[31]Excerpts of an Interview of Lieutenant General Paul E. Menoher, Jr., in Robinson, 50.

[32]Dep't of the Army, TRADOC Pamphlet 525-69, Concept of Operations, (1 Aug 95).

[33]"Rapid Technology Growth Spawns Land Information Warfare Activity," Signal July 1996: 54.

[34]"Rapid Technology," 51.