NAVAL WAR COLLEGE
Newport, R.I.

COMPUTER NETWORK ATTACK VERSUS OPERATIONAL MANEUVER FROM THE SEA

by

Dale W. Herdegen
Major, USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the department of Joint Military Operations.

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

Signature:

8 February, 2000

Professor Gerry Dillon
CDR Erik Dahl, USN

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): COMPUTER NETWORK ATTACK VERSUS OPERATIONAL MANEUVER FROM THE SEA (U)	
9. Personal Authors: Dale W. Herdegen, MAJOR, USMC	
10.Type of Report: FINAL	11. Date of Report: 8 February 2000
12.Page Count: 24	12A Paper Advisor (if any):

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:
COMPUTER, NETWORK, OPERATIONAL, MANEUVER, MAGTF, MARINE CORPS, CNA, CND, ATTACK, DEFENSE

15.Abstract:

Operational Maneuver From The Sea (OMFTS) combined with the Marine Corps' use of mission command and control is a powerful and enabling concept. However, OMFTS and its reliance on information and information systems leaves the Marine Air-Ground Task Force (MAGTF) vulnerable to computer network attack (CNA).

Mission command and control can reduce the impact of the loss of command and control, but it can not overcome the vast and complex array of threats presented by CNA. Protection against CNAs exists and is implemented through a four step process of protect, detect, restore, and respond.

Education and training are the key ingredients to survival in the information age.

16.Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17.Abstract Security Classification: UNCLASSIFIED	
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19.Telephone: 841-6461	20.Office Symbol: C

Security Classification of This Page Unclassified

Abstract of

COMPUTER NETWORK ATTACK VERSUS OPERATIONAL MANEUVER FROM THE SEA

Operational Maneuver From The Sea (OMFTS) combined with the Marine Corps' use of mission command and control is a powerful and enabling concept. It amplifies Marine Corps combat power by coupling maneuver warfare with technological advances in speed, mobility, fire support, communications, and navigation to rapidly identify and exploit enemy weaknesses. OMFTS facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection. However, OMFTS and its reliance on information and information systems leaves the Marine Air-Ground Task Force (MAGTF) vulnerable to computer network attack (CNA).

Mission command and control can reduce the impact of the loss of command and control, but it can not overcome the vast and complex array of threats presented by CNA. Protection against CNAs exists and is implemented through a four step process of protect, detect, restore, and respond. Protection starts with a vulnerability assessment and ends with inoculation after a successful attack. However, protection is never assured.

The Marine Corps can reduce its vulnerability to CNAs by establishing an Information Warfare specialty, training all Marines in basic network defense, and providing detailed education and training for information system operators and system administrators. Finally, CNAs must be incorporated into exercises to illustrate the inherent vulnerabilities in information systems and to practice protective measures.

"Increasing reliance on automated information systems is a JTF's Achilles Heel..."

MCWP 6-23

THESIS

To execute Operational Maneuver From the Sea (OMFTS) with its emphasis on technology and information systems, the MAGTF is dependent on the information and information services provided by the Defense Information Infrastructure (DII), the National Information Infrastructure (NII) and the Global Information Infrastructure (GII).[1] Extensive connections to and reliance on computer networks and civilian communication systems opens the MAGTF up to a variety of new and different threats and threat sources from points around the world.[2] Individuals, organized groups, countries, multinationals, and intelligence organizations can exploit this reliance using Computer Network Attacks (CNAs) to strike the MAGTF.[3]

The hypothesis of this paper is that OMFTS combined with the Marine Corps' use of mission command and control makes the Marine Air-Ground Task Force (MAGTF) resistant to Computer Network Attack (CNA). To support the hypothesis, this paper will examine: first, the relationship between OMFTS and information systems and infrastructure; second, the CNA threats to the MAGTF; third, the vulnerabilities of a MAGTF to CNA; fourth, computer network defenses countering MAGTF vulnerabilities; and fifth, how mission command and control neutralizes CNAs. Finally, the paper ends with conclusions and recommendations.

INTRODUCTION

To defeat the MAGTF, an opponent must strike at its operational Center of Gravity (COG).• The operational COG is derived from the MAGTF's critical strengths; ground forces,

• Attacking the strategic center of gravity may also defeat the MAGTF. Generally, such an attack would be against the will of the U.S. and is beyond the scope of this paper.

air forces, combat service support, maneuver warfare, and technology. The MAGTF's operational center of gravity is the critical strength from which it derives the majority of its combat power. For the MAGTF, the operational COG generally shifts between the air and ground forces according to the mission.

OMFTS and maneuver warfare make it very difficult for an opponent to strike directly at the MAGTF's operational COG: Confronting the full combat power of a MAGTF can be very costly. Rather, an opponent must attack the MAGTF through a critical vulnerability--a critical strength or critical weakness through which the operational center of gravity may be defeated. Tracing backwards, you can determine that MAGTF combat power is amplified by its maneuver. Maneuver is supported by command and control, and command and control is supported by information and information systems. To the extent that these elements are tied together, information and information systems may be the thread that unravels the MAGTF's combat power. Mission command and control loosens the ties to information systems. Is it capable of protecting the MAGTF against CNA in OMFTS?

OMFTS AND INFORMATION SYSTEMS AND INFRASTRUCTURE

Traditionally, a MAGTF transfers command and control from the ship to the shore. The infrastructure supporting the transition is developed in stages. Single channel radio provides the principal means of communications with a landing force in the early stages of an operation. As the operation evolves, local area networks (LANs) and Switched Backbone (SBB) networks provide the information transfer requirements of command and control. Maneuver battalions continue to depend mainly on SCR throughout the operation.[4]

The traditional picture changes with Operational Maneuver From The Sea (OMFTS) and its implementation of maneuver warfare. OMFTS emphasizes speed and tempo and demands compressed planning, decision, execution, and assessment cycles.[5] OMFTS uses the sea as a maneuver area to project naval expeditionary power directly against an exposed enemy center of gravity or critical vulnerability while avoiding obstacles and strong points. Fire support, command and control, and logistics functions remain largely at sea to reduce the footprint ashore. Successful maneuver which requires a real-time knowledge of friendly and enemy positions is provided for through the common operational picture (COP) shared throughout the amphibious task force and the landing force.[6]

To support the information transfer requirements associated with OMFTS, the MAGTF is increasing dependent on rapidly evolving technologies and relies on the globalization of networked communications.[7] The networked communications include the Global Information Infrastructure (GII), the National Information Infrastructure (NII), and the Defense Information Infrastructure (DII) which are vast, complex sets of information systems supported by commercial grids and infrastructure.[8]

The MAGTF also relies on information and information systems to support command and control, logistics, fire support and the other battlefield functions. "[W]arfighters depend upon information to plan operations, deploy forces, and execute missions."[9] OMFTS amplifies this information dependence by striving for an increased operational tempo.[10] Data must be received, processed, and transferred at a speed for which sustained manual operations are either inadequate or inappropriate at the operational level of war. Information systems are thus required to support the flow of information.

The current level of information technology reliance coupled with the inchoate threat provides only minor linkage to the MAGTF's COG. However, as the quest to increase the tempo and efficiency of operations continues, command and control on the revolutionized battlefield will increasingly depend on information and information systems. When the MAGTF can no longer conduct OMFTS operations without the constant and uninterrupted aid of information systems, then information systems become a critical vulnerability exploitable by hostile forces.[11]

THREATS

> *"We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers."*
>
> John M. Deutsch, Former Director, CIA*
> Washington Post, 26 June 1996

Under the OMFTS concept, a deployed MAGTF still faces a traditional C2W threat. Meaconing, Intrusion, Jamming, and Interception (MIJI) are developed and practiced capabilities among potential opponents. These traditional threats are addressed with traditional means; physical security, operations security, counter deception, counter intelligence, and electronic protection measures that are incorporated in plans and exercises. However, the communication architecture supporting OMFTS does reduce some of the traditional C2W threat to the MAGTF by basing functional area support on sea platforms. Operating information systems at sea reduces the threat from physical destruction, jamming, and intrusion. The added distance from a potential enemy provides a shield against direct attack.

* Mr. Deutsch also provides an example of a vulnerability through lack of human understanding. He admittedly used his home computer to process compartmentalized information then used that same computer to connect to the internet.

On the other hand, with OMFTS, the MAGTF is dependent on the information and information services provided by the Defense Information Infrastructure (DII) which is highly susceptible to attack.[12] The extent of connections within the GII, NII, and DII opens the MAGTF up to a variety of new and different threats and threat sources from points around the world.[13] Individuals, organized groups, countries, multinationals, and intelligence organizations can strike the MAGTF from around the globe.[14]

"The threats to the information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing, [and] come from those motivated by military, political, social, cultural, ethnic, religious, personal, or economic gain."[15] The threat goes beyond hackers and involves terrorist, national, and transnational groups that directly target the United States. The MAGTF can expect potential adversaries to use CNA as an inexpensive and possibly surgical strike method to attack a critical vulnerability or tactical, operational, or strategic center of gravity.[16]

The means to conduct an attack against the MAGTF are readily available. "[A] Third-world nation can procure a formidable, modern IW capability virtually off the shelf."[17] With this arsenal of cyber weapons, "Even marginal foes can take on a superpower that no longer can be challenged with conventional weapons," said former Senator Sam Nunn.[18] Using the DII, an opponent can inflict damage on information or information systems vital to the MAGTF from virtually any location.[19] Vice-Chairman elect of the Joint Chiefs of Staff, Gen. Richard Myers warns that other countries consider cyber attack a way of overcoming the disparity in conventional forces and neutralizing the United States.[20] These attacks can degrade the MAGTF commander's ability to make sound and timely decisions, prevent resupply, change critical data,

or shut down entire networks.[21] The MAGTF's vulnerabilities to these threats are addressed next.

VULNERABILITIES

Marine Corps tactics, techniques, and procedures as well as the tactical communications architecture are rapidly evolving to meet the information transfer requirements of OMFTS, but implementation of new technology has outpaced the MAGTF's ability to protect her vital systems.[22] OMFTS and its reliance on technology and computer networks create vulnerabilities that must be addressed.[23] The complexities of the connections and the sheer volume of components make it impossible to protect everything connected to a computer network.[24] Vulnerabilities exist in both the information infrastructure and in information systems. They exist from insiders, in defective hardware and software, and in software designed with backdoors which purposely create security loopholes. Vulnerabilities can be injected when purchasing new equipment, through hardware and software upgrades, and during network installation or reconfiguration. Nothing is completely protectable.[25] "This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure."[26]

Clarifying the danger, Red Team—computer and network experts posing as the enemy--CNAs were conducted during a series of exercises named Eligible Receiver. These attacks showed the devastating and degrading capabilities of CNA. Furthermore, they proved the vulnerabilities in the architecture to the National Command Authorities.[27]

The Pentagon now spends about a billion dollars a year defending its networks. However, an estimated 80 to 100 successful intrusions daily underscore the continued

vulnerability of its computer systems.[28] The MAGTF relies on these systems for operation planning and execution and connects to these systems when deployed.

With computer networks, the weakest link generally determines the overall network vulnerability. Some argue that regardless of the precautions taken that there is no such thing as a 100 per cent secure network[29] and warn that internet security is unfixable.[30] "Skilled hackers are much more capable than you think. The more defenses you have, the better. And yet [your defenses] still won't protect you from the determined hacker."[31] Powerful and malicious hackers can find a way around every protection. Many can completely take over a compromised system.[32] Michael Vatis, America's top cyber-cop who heads the FBI's National Infrastructure Protection Center, says that most incidents currently involve disgruntled employees who sabotage computer systems for revenge or crooks who use the internet for scams and fraud. "There is currently no effective way to police cyberspace."[33]

While scams and fraud may not directly impact the MAGTF, they are indicative of the vulnerabilities in the commercial systems supporting command and control and the other functional areas. Furthermore, potential adversaries are using technologies readily available[34] to build information warfare capabilities in support of espionage.[35] These capabilities pose a direct threat to the MAGTF.

The exploitable vulnerabilities for a MAGTF are broadly based upon or categorized into personnel, infrastructure, or data. Vulnerabilities based upon personnel include physical destruction, information overload, over-reliance or over-confidence in the system•, misinformation, lack of human understanding, failure to accept and utilize available computer security safeguards, and enemy non-sophistication.[36] The most exploitable of personnel

• The over-confidence of the Germans in WWII on the enigma machine is a good example of this.

vulnerabilities is that users view network protection as awkward or unnecessary, thus they fail to understand their role in cyberspace security.[37] Furthermore, lack of technical proficiency or training leads to a reliance on civilian contractors or changes the system from a work reducer to a work producer.[38] One of the most difficult command and control issues currently facing the Marine Corps is supporting a MAGTF with qualified computer and information system personnel and equipment.[39] However, the most dangerous of these vulnerabilities to the MAGTF is over-reliance. Since any information system is vulnerable to attack, over-reliance coupled with system corruption or failure can lead to command and control paralysis.

The next set of vulnerabilities concerns the infrastructure. They include physical destruction of equipment, disruption, monitoring, penetration, complicated functioning, and mechanical breakdown or systematic failure. "The DII is highly susceptible to attacks which disrupt information services (availability) or corrupt the data (integrity) within the infrastructure. Many nations and groups have the capability to cause significant disruption to the DII and, in turn, cripple operational readiness and military effectiveness."[40]

The final vulnerabilities are based upon data. These include denial, interruption, corruption, spoofing, data exploitation, theft, or destruction. Attacks on data can be the hardest to detect and are the most malicious and disruptive to operations. The types of data attacks vary with the imagination of the perpetrator. These attacks vary in detectability and impact and could include such events as fake e-mail messages supporting psychological operations, altered supply data that impacts repair parts, stolen operational plans, or a corrupted file that destroys your brief the to MAGTF commander that starts in five minutes.

Computer Network Attack is countered by Computer Network Defense (CND). The next section articulates defenses designed to protect the data and the infrastructure.

COMPUTER NETWORK DEFENSE

Computer Network Defense (CND) is supported by four interrelated processes; environment protection, attack detection, capability restoration, and attack response. The MAGTF is supported in these processes by defense agencies through policies, procedures, assessments, and advice. The coherency of the support is steadily increasing. Last year, the United States Space Command established the world's first cyber warfare task force for CND. Later, an offensive unit will join the fray using computer keyboards and modems as its weapons.[41] Despite the abundance of available help, the MAGTF retains primary responsibility for protection of its information environment.

> *"The force that best controls, manipulates, and safeguards information and information systems will enjoy a decided military advantage..."*
>
> *-- A Concept for Information Operations*

The first step in the process is environment protection. The minimum level of environment protection is established by DOD Directive 5200.28.[42] Additional protection measures are incorporated based upon a required vulnerability assessment.[43] A threat assessment should also be conducted. Vulnerabilities are based on system components and architecture while threats are based upon adversary intent and capabilities. Following these assessments, additional protective measures are implemented based upon a cost-benefit analysis.[44] Too little protection puts the mission at risk. Too much protection degrades mission accomplishment.[45] Vulnerability and threat factor into the benefit parameter.[46] Costs include: slower performance, decreased reliability, and decreased accessibility[47]

There are tools and agencies available to assist the MAGTF in conducting a vulnerability assessment. For the self-motivated, RAND has produced a matrix with which categorizes vulnerabilities into twenty separate types then provides security techniques to address the

vulnerabilities.[48] The vulnerability/security technique pairs are then divided into another matrix that provides a simple cost-benefit analysis. Professional help is available through the Fleet Information Warfare Center (FIWC) that will assist in identifying system vulnerabilities and will provide Red Teams in support of military operations.[49]

The second step in the process of CND is attack detection. This action relies on; human detection by system administrators and users; automated detection with built-in or add-on hardware and software; and Indications and Warnings (I&W) through law enforcement agencies, intelligence, and information warfare centers. Attack detection is a cooperative effort that is the key to the next two steps in the process; capability restoration and attack response.[50]

Capability restoration is the third step in the process of CND. It is inevitable that the MAGTF will experience attacks against its information systems. The key to maintaining operational momentum is recovering quickly or finding an alternate means of accomplishing the mission. Again consider three areas: personnel, infrastructure, and data. Personnel must understand alternate methods of accomplishing the mission if the primary information system is attacked. The infrastructure must be redundant and resilient enough to withstand the effects of enemy action as well as environmental phenomena, and the data must be reliable, replaceable, and recoverable.[51] The tool that addresses these issues and allows for quick recovery is a Continuity Of Operations Plan (COOP) that strategically addresses issues pertinent to the ongoing mission. The COOP details actions for immediate recovery and long term sustainment of the information systems and architecture. When immediate system recovery is impossible, alternate means of mission accomplishment should be identified.[52]

Additional recovery assistance is available through Computer Emergency Response Teams (CERTs). The Naval Computer Incident Response Team (NAVCIRT), part of the FIWC,

serves as the Marine Corps primary computer incident response capability. NAVCIRT provides assistance in identifying, assessing, containing, and countering incidents that threaten MAGTF information systems and networks and will attach teams to assist during military operations.[53]

The final step in the CND process is attack response. An attack against the MAGTF information infrastructure will trigger a riposte based upon the current level of hostilities. The response could be a combination of law enforcement, diplomatic actions, economic sanctions, or military force.[54] An effective parry requires that all users and support personnel be aware of the indicators and the procedures to be followed in the event of an attack.[55] A crucial final step is to determine why the attack was successful and then inoculate against future attempts.[56]

To support the process of protection, detection, restore, and respond, the Marine Corps has established the Marine Corps Command Center and the Network Operations Center (NOC). The NOC has the overall responsibility of *managing* any computer intrusion incidents and coordinates with the FIWC which is the single point of contact for *monitoring* the security of information systems.[57]

The combination of these agencies, support teams, policies, and procedures may do well to detect and reduce the effect of CNAs, but they can not eliminate them. The next section investigates the role that mission orders play in negating CNAs and allowing the MAGTF to continue operations if its systems are disrupted.

MISSION COMMAND AND CONTROL

> *"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. Of you try to hold everything, you hold nothing."*
>
> Frederick the Great
> Quoted in Foertsch, The Art of Modern War, 26 June 1996

The Marine Corps command and control concept is based upon the timeless fundamentals of war that account for an animate, interfering enemy. The concept is technology independent and uses commander's intent and the desired end state to guide subordinate action.[58] A subordinate commander's initiative overcomes loss of command and control while speed and agility overcome precision and certainty.[59] While maneuver warfare is used to shatter the enemy's moral, mental, and physical cohesion, mission command and control allows Marines to operate in an uncertain, chaotic, fluid environment with limited external support. Thus, based on the concept of mission command and control, the MAGTF can continue to operate, at least temporarily, during a CNA that denies the use a command and control network.[60]

Denial is the only form of CNA attack useable against encrypted command and control networks. Denial includes jamming the network or destroying or disrupting the communication architecture. CNA attacks such as spoofing, sniffing, hacking, or inserting malicious code are prevented by the encryption.• Additionally, denial attacks create a loss-of-service that is noticeable by the operators and network administrators. Immediate action to respond and recover further negates the effects of denial attacks against an encrypted command and control system. Therefore, CNA attacks against encrypted MAGTF command and control systems are not a critical vulnerability unless there is long-term loss of service.

On the other hand, not all systems supporting the MAGTF are encrypted: administration functions, some logistics functions, and e-mail rely on connections to unencrypted networks. Unencrypted systems are vulnerable to CNAs that are more subtle and harder to detect. These support functions are not protected against spoofing and other forms of data manipulation in which the network continues to operate but sends false or misleading signals. Attacks against

support systems are generally slower to culminate but can be severely disruptive. These attacks could target; logistics to change supply requests or reroute parts, intelligence by providing false or misleading information on unclassified systems, the mind of the commander using direct psychological attacks via e-mail, or the moral of the troops by zeroing out automatic deposits or deleting monthly allotments. The list of attacks is limited only by the imagination, training, and intelligence support of an opponent. Mission command and control can not protect against these attacks.

Thus, mission command and control supports CND negate temporary denial attacks against command and control systems on encrypted systems but can not negate more malicious and less detectable attacks against unencrypted systems. Depending on the type and extent of the mission, a critical vulnerability may exist.

RECOMMENDATIONS

"If at first the idea is not absurd, then there is no hope for it."

Albert Einstein

To address vulnerabilities and threats, the MAGTF must be organized, trained, and equipped to plan and execute CND in support of OMFTS.[61] The Marine Corps has taken the first steps and incorporated CND in the broader context of Information Operations (IO) in doctrinal publications, tactics, techniques, and procedures. Furthermore, the Marine Corps has called for the integration of IO within the context of the Marine Corps' OMFTS-based warfighting strategy and the Marine Corps planning process.[62]

• Encryption does not prevent insider attacks which could include the whole array of CNAs.

To complete the integration of IO into the Marine Corps' warfighting philosophy, the Marine Corps must make organizational changes. With the same vigor that every Marine is a rifleman, every Marine must be an information warrior. While yearly qualification on the computer network and a crossed-keyboards badge seems comical, they may not be far off. Last year, all Marines that did or might touch a computer system were required to receive a security certification (the qualification?) that was recorded in their official record (the badge?). Did the future just get a little closer?

In addition to making every Marine an information warrior, the Marine Corps needs to identify, train, and equip personnel for a new combat arms specialty, Information. The first step was taken with the integration of the data and communications specialties. The process continued with the complete weaving of information systems into the warfighting functions and with the integration of IO into the Marine Corps' warfighting philosophy. The Marine Corps needs to continue the course.

In the near term, the Marine Corps must focus on education and training. They are the key ingredients to survival in the information age. Information systems are becoming highly sophisticated weapon and combat support systems. Advanced education is required to operate, understand, manipulate, and protect these systems. A jet pilot is educated for two years before becoming combat ready; a command and control system 'pilot' is merely shown how to log on and is expected to learn on the job. Many system administrators—the main line of defense—receive a similar degree of training. To step forward into the information age, structured and detailed education for information systems is required.

Training begins where education leaves off and should be tailored to the billet. First, all Marines should receive basic CND training to reduce successful human engineering attacks in

which users are tricked into revealing passwords or allowing unauthorized system access. Basic training should also increase threat awareness to reduce vulnerabilities due to laziness or lack of understanding which lead to failure to use available safeguards. Next, system operators should receive additional training that supports the processes of attack protection, detection, restoration, and response. Finally, system administrators need to be incorporated into the IO organization and should receive detailed training in CND.

Training must be incorporated into exercises. Realistic training will develop the skills required to overcome a computer network attack and continue to operate with degraded or inoperative information systems. To facilitate this, MAGTF exercises should include Red Teams that are allowed to aggressively attack and exploit weaknesses in the MAGTF's information systems. These attacks will compel Marine forces to overcome the inevitable failure of their information systems.[63]

Finally, the Marine Corps, in concert with the rest of the Department of Defense, should continue the migration of all possible systems onto encrypted networks based upon a cost-benefit analysis. Again, this will reduce availability of these systems to some valid users, but the move will add another layer of protection against many forms of CNA.

CONCLUSION

OMFTS combined with the Marine Corps' use of mission command and control is a powerful and enabling concept. It amplifies Marine Corps combat power by coupling maneuver warfare with technological advances in speed, mobility, fire support, communications, and navigation to rapidly identify and exploit enemy weaknesses. OMFTS facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection.[64]

However, OMFTS and its reliance on information and information systems still leaves the MAGTF vulnerable to computer network attack—not just to the physical destruction of equipment and personnel, but also to exploitation and disruption through data manipulation, spoofing, hacking, and other aspects of computer network attack.[65] Mission command and control can reduce the impact of the loss of command and control, but it can not overcome the vast and complex array of threats presented by CNA.

Protection against CNAs exists and is implemented through a four step process of protect, detect, restore, and respond. Protection starts with a vulnerability assessment and ends with inoculation after a successful attack. Nevertheless, even with the best protection, networks will be vulnerable to CNA. Furthermore, networks will be increasingly targeted since information and information technology are no longer simply enhancements to warfare, but military objectives.[66]

The Marine Corps can reduce its vulnerability to CNAs by establishing an Information Warfare specialty, training all Marines in basic network defense, and providing detailed education and training for information system operators and system administrators. Finally, CNAs must be incorporated into exercises to illustrate the inherent vulnerabilities in information systems and to practice protective measures.

NOTES

[1] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), 25.

[2] U.S. Marine Corps, Concept for Information Operations (Quantico, VA: August 1998), A-2.

[3] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), B-6.

[4] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 5-2.

[5] Ibid, 1-1.

[6] Ibid, 8-3.

[7] U.S. Marine Corps, Concept for Information Operations, (Quantico, VA: August 1998), A-7.

[8] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), 25.

[9] Joint Chiefs of Staff, Defensive Information Operations Implementation (CJCSI 6510.01B) (Washington, D.C.: August 22, 1997), A-1.

[10] U.S. Marine Corps, United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA: n.d.), I-9-I-22.

[11] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 7-6.

[12] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), 31.

[13] U.S. Marine Corps, Concept for Information Operations (Quantico, VA: August 1998), A-2.

[14] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), B-6.

[15] U.S. Marine Corps, Concept for Information Operations (Washington: August 1998), A-2.

[16] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), 24.

[17] Ibid, ES-5.

[18] Stephen Green, "Pentagon, Once Stung, Beefs up Cyberwarfare Role", The San Diego Union-Tribune, 24 December 1999, A-1.

[19] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 7-6.

[20] "U.S. Military Adds Cyber Tactics to its Attack Arsenal," The Toronto Star, 6 January 2000, Lexis-Nexis, (13 January 2000).

[21] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 1-1.

[22] Ibid, 5-1.

[23] U.S. Marine Corps, United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA: n.d.), I-9 – I-22.

[24] Joint Chiefs of Staff, Information Operations (Joint Pub 3-13) (Washington, D.C.: October 9, 1998), III-1.

[25] Robert H. Anderson and others, Securing the U.S. Defense Information Infrastructure: A Proposed Approach (Washington: RAND 1999), 10.

[26] William M. Daley, Commerce Secretary quoted in Marc Lacey, "Clinton Outlines Plan and Money to Tighten Computer Security," New York Times, 8 January 2000, A-14.

[27] Stephen Green, "Pentagon, Once Stung, Beefs up Cyberwarfare Role," The San Diego Union-Tribune, 24 December 1999, A-1.

[28] Ibid.

[29] Ting Ting Lee, "Covering All Aspects of Network Security," New Straits Times (Malaysia), 2 December 1999, Lexis-Nexis, (13 January 2000).

[30] Robert H. Anderson and others, Securing the U.S. Defense Information Infrastructure: A Proposed Approach (Washington: RAND 1999), 25.

[31] "Security for All-Intrusion Detection Systems Explained," Bangkok Post, 3 November 1999, Lexis-Nexis, (13 January 2000).

[32] Bob Drogin, "U.S. Scurries to Erect Cyber-Defenses; Security: At Threat Rises, Government Task Force Prepares for Internet Combat," Los Angeles Times, 31 October 1999, A-1.

[33] John Arqilla and David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age (Washington: RAND 1997), 239.

[34] U.S. Marine Corps, Concept for Information Operations (Quantico, VA: August 1998), A-2.

[35] Bob Drogin, "U.S. Scurries to Erect Cyber-Defenses; Security: At Threat Rises, Government Task Force Prepares for Internet Combat," Los Angeles Times, 31 October 1999, A-1.

[36] U.S. Marine Corps, Command and Control,(MCDP 6) (Washington, D.C.: 4 October 1996), 79.

[37] John Arqilla and David Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age (Washington: RAND 1997), 240.

[38] Capt Christopher S. Bey, "Chasing our Tail: The Quest and Costs for Information Dominance", Marine Corps Gazette, October 1998, 19.

[39] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 1-1.

[40] Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield (Washington: October 1994), 31.

[41] Roger Dobson, "The Hacker Goes to War," Sunday Times (London), 12 December 1999, Lexis-Nexis, (13 January 2000).

[42] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 7-7.

[43] Joint Chiefs of Staff, Defensive Information Operations Implementation (CJCSI 6510.01B) (Washington, D.C.: August 22, 1997), C-10.

[44] U.S. Marine Corps, Information Assurance (MCO P5239.1) (Washington, D.C.: DRAFT), 7.

[45] Ibid, 8.

[46] U.S. Marine Corps, United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA: n.d.), IX-13.

[47] Robert H. Anderson and others, Securing the U.S. Defense Information Infrastructure: A Proposed Approach (Washington: RAND 1999), 74.

[48] Ibid, 48-59.

[49] U.S. Marine Corps, Information Assurance (MCO P5239.1) (Washington, D.C.: DRAFT), 32.

[50] Joint Chiefs of Staff, Information Operations (Joint Pub 3-13) (Washington, D.C.: October 9, 1998), III-10.

[51] U.S. Marine Corps, Concept for Information Operations (Washington: August 1998), A-4.

[52] U.S. Marine Corps, Information Assurance (MCO P5239.1) (Washington, D.C.: DRAFT), 23.

[53] Ibid, 27.

[54] Joint Chiefs of Staff, Information Operations (Joint Pub 3-13) (Washington, D.C.: October 9, 1998), III 14-15.

[55] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 7-9.

[56] Robert H. Anderson and others, Securing the U.S. Defense Information Infrastructure: A Proposed Approach (Washington: RAND 1999), 72-74.

[57] U.S. Marine Corps, Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998), 7-9.

[58] U.S. Marine Corps, Command and Control,(MCDP 6) (Washington, D.C.: 4 October 1996), 79.

[59] Ibid, 135.

[60] Ibid, 79.

[61] U.S. Marine Corps, Concept for Information Operations (Quantico, VA: August 1998), A-2.

[62] U.S. Marine Corps, Concept for Information Operations (Quantico, VA: August 1998), A 9-10.

[63] U.S. Marine Corps, Concept for Information Operations (Quantico, VA: August 1998), A 9-10.

[64] U.S. Marine Corps, United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA: n.d.), IX-18.

[65] U.S. Marine Corps, United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA: n.d.), IX-18.

[66] U.S. Marine Corps, Concept for Information Operations, (Quantico, VA: August 1998), A-10.

BIBLIOGRAPHY

Anderson Robert H. and others. Securing the U.S. Defense Information Infrastructure: A Proposed Approach (Washington: RAND 1999).

Arqilla, John and David Ronfeldt. In Athena's Camp: Preparing for Conflict in the Information Age (Washington: RAND 1997).

Bey, Capt Christopher S. "Chasing our Tail: The Quest and Costs for Information Dominance". Marine Corps Gazette. October 1998, 18-20.

Defense Science Board Summer Study Task Force. Information Architecture for the Battlefield (Washington: October 1994).

Dobson, Roger. "The Hacker Goes to War." Sunday Times (London). 12 December 1999, Lexis-Nexis. (13 January 2000).

Drogin, Bob. "U.S. Scurries to Erect Cyber-Defenses; Security: At Threat Rises, Government Task Force Prepares for Internet Combat." Los Angeles Times. 31 October 1999, A-1.

Green, Stephen. "Pentagon, Once Stung, Beefs up Cyberwarfare Role." The San Diego Union-Tribune. 24 December 1999, A-1.

Lacey, Marc. "Clinton Outlines Plan and Money to Tighten Computer Security." New York Times. 8 January 2000, A-14.

Lee, Ting Ting. "Covering All Aspects of Network Security." New Straits Times (Malaysia). 2 December 1999. Lexis-Nexis. (13 January 2000).

"Security for All-Intrusion Detection Systems Explained." Bangkok Post. 3 November 1999. Lexis-Nexis. (13 January 2000).

Joint Chiefs of Staff. Defensive Information Operations Implementation (CJCSI 6510.01B) (Washington, D.C.: August 22, 1997).

Joint Chiefs of Staff. Information Operations (Joint Pub 3-13) (Washington, D.C.: October 9, 1998).

U.S. Marine Corps. Command and Control (MCDP 6) (Washington, D.C.: 4 October 1996).

U.S. Marine Corps. Communication and Information Systems (MCWP 6-22) (Washington, D.C.: November, 1998).

U.S. Marine Corps. Concept for Information Operations (Quantico, VA: August 1998).

U.S. Marine Corps. Information Assurance (MCO P5239.1) (Washington, D.C.: DRAFT).

U.S. Marine Corps. United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA: n.d.).

"U.S. Military Adds Cyber Tactics to its Attack Arsenal." The Toronto Star. 6 January 2000. Lexis-Nexis. (13 January 2000).