NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

INFORMATION OPERATIONS: THE NEED FOR A NATIONAL STRATEGY

by

Samuel P. Morthland

June 2002

Thesis Advisor: Dr. John Arquilla
Second Reader: Prof. Daniel Boger

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Information Operations: The Need for a National Strategy			**5. FUNDING NUMBERS**
6. AUTHOR(S) Morthland, Samuel P.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

This thesis explores the hypothesis that a national information strategy would enhance military effectiveness and national security. Analysis of the role of information in conflict, a definition of what information is, and how it can be used to support military operations establishes the foundation for the thesis. Perception management, system destruction, and information exploitation are identified as key elements of to an effective strategy. They are reflected in the 17 information operational capabilities in joint doctrine. Four categories were created to differentiate the IO capabilities along offense/defense and technological/cognitive lines. The current focus of IO in the U.S. is the technical/offensive IO category, with less attention being given to the conceptual/ cognitive category. This may be due to a lack of strategic IO planning. Therefore, a planning methodology is developed herein and used to analyze the Administration's response to the terrorist attacks on 9/11/2001. A detailed analysis of the IO capabilities used identified two shortcomings: the failure to identify all key audiences, and not considering all the IO capabilities available. The thesis recommends adopting the concepts of a National Information Strategy and the IO strategic planning methodology used in the study.

14. SUBJECT TERMS Information operations, national security strategy, al Qaeda, terrorist organizations, perception management, information superiority, knowledge			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INFORMATION OPERATIONS: THE NEED FOR A NATIONAL STRATEGY

Samuel P. Morthland
Major, United States Air Force
B.S., Wright State University, 1986
M.S., Embry-Riddle University, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2002

Author: Samuel P. Morthland

Approved by: Dr. John Arquilla, Thesis Advisor

Prof. Daniel Boger, Second Reader

Prof. Gordon McCormick, Chairman
Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the hypothesis that a national information strategy would enhance military effectiveness and national security. Analysis of the role of information in conflict, a definition of what information is, and how it can be used to support military operations establishes the foundation for the thesis. Perception management, system destruction, and information exploitation are identified as key elements of to an effective strategy. They are reflected in the 17 information operational capabilities in joint doctrine. Four categories were created to differentiate the IO capabilities along offense/defense and technological/cognitive lines. The current focus of IO in the U.S. is the technical/offensive IO category, with less attention being given to the conceptual/ cognitive category. This may be due to a lack of strategic IO planning. Therefore, a planning methodology is developed herein and used to analyze the Administration's response to the terrorist attacks on 9/11/2001. A detailed analysis of the IO capabilities used identified two shortcomings: the failure to identify all key audiences, and not considering all the IO capabilities available. The thesis recommends adopting the concepts of a National Information Strategy and the IO strategic planning methodology used in the study.

THIS PAGE INTENTIONALLY LEFT BLANK

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense, or the U.S. Government.

THIS PAGE INTENTIONALLY LEFT BLANK.

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife for her patience and understanding over the past year and a half while I completed this thesis and the program in general. Her support has been the key to my success and happiness.

Special thanks goes to my fellow IO students for their enthusiastic pursuit of new and interesting theories in information. All of our discussions and projects were key to my success at the Naval Postgraduate School and the completion of this thesis.

And finally, I would like to thank Jennifer Duncan, Dr. Arquilla, Prof. Boger, and the SOLIC Faculty for entertaining my sometimes-fanciful thoughts on emerging doctrinal concepts and organizational designs.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Information is strength—knowledge is power.
Anonymous

The Internet has created the perfect anonymous environment for anyone with access to a personal computer and a phone line to manipulate, search, and organize incredible amounts of information in a span of minutes and communicate with anyone else in the infosphere at the same time. Near total anonymity for anyone is possible through the use of free email hosting sites, anonymizer sites, and the thousands of cyber cafés around the world that offer cheap Internet access to anyone who can pay for a cup of coffee. Add the availability of virtually unbreakable encryption, and the Internet provides an ideal covert command and control communications network. Most importantly, the terrorists of the world know this.

George Tenet, the Director of Central Intelligence, testified to Congress that they had evidence that al Qaeda was using the Internet for command and control since 1998 (Tenet, 2000). He went on to further say,

> terrorists also are embracing the opportunities offered by recent leaps in information technology. To a greater and greater degree, terrorist groups, including Hizballah, HAMAS, the Abu Nidal organization, and Bin Ladin's al Qaeda organization are using computerized files, e-mail, and encryption to support their operations (Tenet, 2000)

It is highly probable the Internet was a source of operational data and the primary means of command and control for al Qaeda. Somehow, they managed to keep their communications and specific plans from U.S. intelligence services for more than five years prior to the attacks on September 11, 2001 (“Terror Plot”, 2001). This is not to say that al Qaeda executed everything perfectly nor did their people keep quiet during questioning following other terrorist attacks. In fact, the U.S. received warnings as early as 1995 about terrorists taking flight lessons in the U.S. with the intent to hijack an aircraft and, in one example, crash it into the CIA building in Washington, D.C. But for some reason the U.S. intelligence agencies failed to share and collaborate on this information and “connect the dots” to prevent the September 11th attacks (“September 11

warnings", 2002). Nor did they step up their monitoring of al Qaeda activity on the Internet.

Most people would be shocked at the kind and amount of information available on the Internet. But the information in and of itself is not the problem. The problem is the ease of gathering detailed information on virtually any subject or profession. Internet search engines find and compile the data, then the terrorists put the data into context, and use it to gain an operational advantage. A small sample of the kind of information available is found in Table 1. It lists the web sites, information available on each site, and how it could have helped terrorists plan the attack.

The ability of al Qaeda to gather operational information, covertly communicate, and transfer funds using hawalas (an ancient Middle Eastern financial network built on trust), should be a wake up call to America of the importance of connectivity.

Table 1. Planning web sites.

Web Site	Information	Potential Use
Airline	Flying Schedules	Synchronize Attack
	Seat Assignment	Sit near critical areas of aircraft like crew cabin door and galleys
FAA	Flight Progress	Command and Control of supporting activities
	Flight Routes	Time route timetables to hijack planes
	Approach Plates	Hijacker to follow normal flight path (i.e., to Washington Reagan)
Aeroplanner	Flight planning information	Create full plans and calculate flight times and turn around points
Defense Link	Pentagon Layout	Decide which side to attack
	Briefing times, etc.	Greater terror impact
Architectural	World Trade Center Construction Details	Able to determine where and how to hit the structure based on construction
White House	Announced Briefings	Could time attack to ensure President was in residence

A. THE FUTURE OF INFORMATION WARFARE IS NOW

What war will look like in the information age has been greatly debated over the past 15 years. Visions of future warfare run the spectrum from a highly automated

version of today, with more unmanned equipment, to a world where the military is only involved on the periphery as individuals, large commercial conglomerates, and other organizations fight over ideas and knowledge. And many authors still describe the advent of information warfare as a point sometime in the distant future. But Arquilla and Ronfedt mention that a type of information warfare, netwar, has been occurring for years now, it just hasn't been classified as such. They offer Radio and TV Martí broadcasts from America to Cuba and the pro-Cuban press as an example of the battle of ideas in the infosphere (Arquilla & Ronfedt, 1997, p. 28).

In the future, information will rise in importance to a point where "the possession and manipulation of information itself can be a key element of the war-winning equation" (Air Force Doctrine Document (AFDD) 2-5, Aug 1998). The Chinese demonstrated their understanding of this principle when they created a three dimensional graphic depicting an aggressive EP-3 turning into a passive Chinese fighter and released it to the world within 24 hours after the incident. The U.S. was then left to explain the video away. Consider the amount of time and effort the U.S. spent refuting it. What would world opinion have been if the U.S. had released a short video or simulation first? Or even at the same time? It is imperative for the U.S. to develop an understanding of information warfare, draft the appropriate doctrine, and reorganize or create new organizations in response to the challenges of information warfare.

James Adams and John Alexander both define information warfare as made up of three pieces: perception management, system destruction, and information exploitation. Each views and uses information differently: "perception management where the information is the message, systems destruction where the information is the medium, and information exploitation where information is an opponent's resource to be targeted" (1998, p. 17; 1999, pp. 105-112). Although both Adams and Alexander use the same model to describe information warfare, they have divergent views on what methods could or should be employed in the future. Reviewing and contrasting their views will provide the spectrum of potential futures in information warfare.

1. Perception Management

Perception management is going to be a critical element in future conflicts in the infosphere, but the question is how is it accomplished with the greatest effect and minimum risk of severe blowback. Alexander advocates using the traditional tools of perception management, psychological operations (PSYOP) and deception, to "win hearts and minds." This would be achieved through the manipulation of and planned deception through the commercial media, military psychological operations, and the Internet to get into and affect minds of our supporters, partners, and enemies (Alexander, 1999, p. 111).

Adams, on the other hand, believes the flow of information in today's networked world cannot be controlled and warns of the consequences of trying to do so. He believes "what should and could be done is to design a new architecture that uses cyberspace and the information revolution to help prosecute warfare". Adams feels any acts of deception have a "limited shelf life" and it would be much better to "tell the unvarnished truth, which has no sell-by date." He argues that the military has to look at unique solutions to emerging situations. For example, rather than targeting the leader of an adversarial country, exploit the opportunities to reach the regular people on the street. Use all avenues of information to give alternatives to the tightly controlled broadcast and print media available in most countries. Convince them why it would be better to change, and if you do it right, they will. Understanding how this kind of information operation could impact "the conduct of military and foreign policy, is something very few in government possess", but is a key to future military conflicts in the information age (Adams, 1998, pp. 274-286).

Adams is correct in saying that false or deceptive information may create a complex situation that is worse than the original conflict. We should change our doctrines to address the "man on the street" and provide him with the truth so he can make an informed decision and act upon it if possible. The only shortcoming in Adam's concept is the lack of the integration of all the tools of perception management.

It is important to realize that directed information campaigns aren't the only ways to engage in perception management. Everything our government does sends one

message or another to our own citizens and the rest of the world. The goal is to anticipate the message an activity will send and make sure it is in alignment with existing policy. For example, consider the message sent by then U.S. Attorney General Janet Reno when she authorized an Immigration and Naturalization Service SWAT team to capture Elian Gonzales, a 6-year-old boy, at 4 o'clock in the morning. The picture in Figure 1 was worldwide on the Internet within 2 hours along with harrowing reports of armed officers in combat gear breaking into a small house and pointing a loaded machine gun at the head of the boy. One can only imagine the damage this act and the associated picture did to the perception of America as the home of the free and brave. Could it have also shattered many Americans' belief that our government protects innocent people? This is the kind of question we need to ask ourselves before every operation so that we continue to project the mental picture we want the world to have of the United States.

Figure 1. Elian Gonzalez Capture. Photograph taken by A. Diaz, the Washington Post, April 22, 2000. Available at http://washingtonpost.com/wp%2Ddyn/photo /topstory/G61939%2D2000Apr22.html

2. System Destruction

Systems destruction is the part of information warfare that targets the actual systems used to transmit and store the information or what is commonly called "the information grid." It is an "interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel" (Miller, Jefferson, & Rogers, 2001, ¶ 6). The grid allows commanders to efficiently collect, process, and disseminate critical information to his forces, but as he becomes

reliant on the grid, the grid becomes a center of gravity that the enemy can target (Libicki & Shapiro, 1999).

While destruction is the easiest function to understand, it is not always required to render an information grid useless. Each node of an information grid or network is built with nodes, like routers, that require software to work properly. It is possible to implant malicious code or viruses in these nodes to slow the network down, delete data, or cause the entire network to crash. This type of destruction or disruption can also happen at a much smaller scale.

Today's smart weapons are computerized marvels that use sophisticated logic to leverage onboard electronic maps and global positioning system (GPS) signals to pinpoint their target. Imagine the operational impact and campaign disruption if an enemy infected those systems with viruses or malicious code, and then at a critical moment in combat activated the virus to render a fighter aircraft, a tank, or an entire ship useless. The Navy got a taste of this potential when a Petty Officer accidentally entered a zero into a database causing the ship's local area network to crash, shutting down all propulsion and leaving the *U.S.S. Yorktown* dead in the water for three hours (Slabodkin, 1998). While embedded viruses in weapons are a frightening concept, imagine how recent conflicts may have changed if the U.S. could have rendered U. S. produced weapons and systems useless when they were used against U. S. interests or forces (Alexander, 1999). Or imagine the consequences if foreign software in U.S. systems "blew up" when used.

Adams looks beyond the "virus in a weapon" tool and is concerned that information technology is moving into every aspect of a military's capability to wage war, from new individual sensing body armor to miniature unmanned combat vehicles to massive "intelligent" databases assisting in command and control decisions. These developing technologies improve the ability to efficiently manage information and deliver force where needed but come at a price, security. The military now relies exclusively on commercially developed technology and develops little specialized technology. It is cheaper and sometimes quicker to use off the shelf technology, but both the hardware and software is vulnerable to manipulation because of the vast numbers of

people involved in its design, production and support. Many software companies use offshore programming houses in India, Singapore, and Russia, and most hardware is produced and assembled outside the United States. Unfortunately, this reliance on the commercial sector will continue to present an information assurance problem, especially in the areas of miniaturization and automation (Adams, 1998).

3. Information Exploitation

Targeting an opponent's operational information, or any form of information, to gain advantage is the third piece of the IW puzzle, information exploitation. Like leading U.S. businesses, the military compiled and automated its massive databases in an attempt to reduce the "fog and friction" on the battlefield and gain information superiority. This centralization of data for command and control is both a boon and a bane. It allows leaders to monitor the battlefield in a level of detail never before imagined.

The common relevant operational picture (CROP) provides the "big picture" of what is happening in very near real time to the senior leadership at all levels and can be used to guide the war. The CROP depends on interoperable systems and the integrated databases, which may now be targets themselves. There are two ways these databases could be corrupted. One way an adversary could access the databases would be through backdoors programmed into the base code of the operating systems. A second way would be to brake into the CROP servers and enter bad data or change the data linkages within the database code. Either could cause the entire system-of-systems could crash like the *U.S.S. Yorktown* mentioned earlier, but someone would have to break into our secure networks to do this. Firewalls, updated software, encryption, biometrics, and other network security measures should keep the data secure. The key assumption is should.

Breaking into secure networks isn't as hard as it used to be. The explosion of the numbers of personal computers, the computational power of the newest processors, free system administration/hacking programs on the Internet, and commercially available network administration/component training all lower the cost of entry and allow nearly anyone to become a dangerous hacker. Business and military leaders need to understand that hackers are no longer bored kids looking for some excitement (Adams, 1998). They are sophisticated systems operators with specific network knowledge who can enter some

of the most secure networks through holes in even the newest security programs. Once inside, they can gain root access and do anything on or to the network (Alexander, 1999).

If hackers can get into a network to just fool around or post a costly but harmless mail-replicating virus, think of the potential damage they pose to essential and sensitive data. If a hacker can do it, so can an adversary. They could use the same techniques to enter your network and either gather information (computer network exploitation (CNE)) or place malicious code to crash the network (computer network attack (CNA)).

B. THESIS OVERVIEW—SCOPE OF THE STUDY

The purpose of this thesis is to explore the idea that a national information strategy would enhance the effectiveness and breadth of military information operations. To fully explore this concept, this thesis will take the following steps. First, it will examine a sample current information operations theory to establish a general foundation for thinking about information operations. Next, it will suggest a planning methodology derived from the foundation information and discuss the linkage of the plan to national strategic, operational, and tactical objectives. Then the thesis will compare the current war on terrorism to the planning methodology and strategy linkages to validate them and evaluate the first months of the IO war effort. Finally, the thesis will conclude with a net appraisal of the benefits to military information operations of a national information strategy and suggest further areas of research.

C. KEY CONCEPTS

Before starting the study of the potential benefits of a national information strategy, we must first establish a basic conceptual foundation. To do this, the following questions will be answered. What is information and why is it important? What are information operations? Why are information operations used? And finally, why a national military information strategy? The answers to these questions set the stage for the study and provide a common conceptual frame of reference and key term definitions.

1. What is information and why is it important?

The core concept for the entire theory of information operations is information. This may sound tautological, but we should discuss what is and isn't information. We will use the cognitive hierarchy found in Joint Publication (JP) 6-0 as a basis of our

discussion with one modification (see Figure 2). We will use the broader definition of information found in JP 1-02 and use information as the foundation of our IO information pyramid and work our way up to understanding.

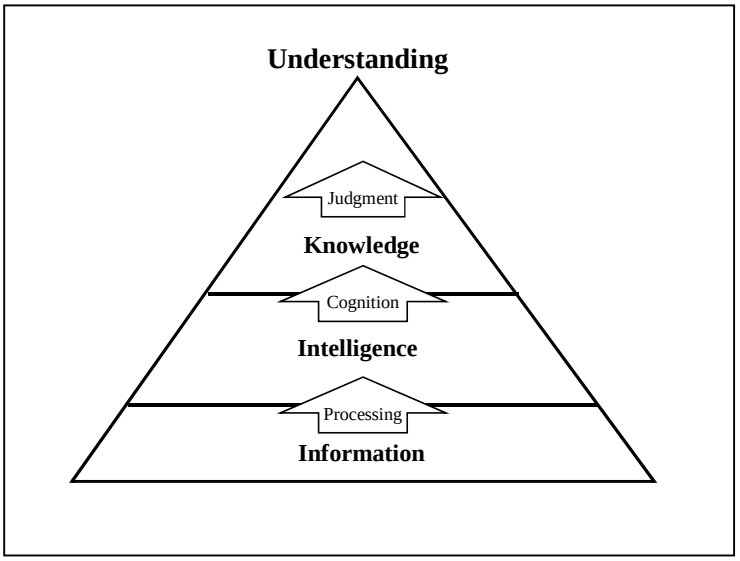

Figure 2. The IO Information Pyramid.

The joint definition of information (see Figure 3) highlights the difference between the two accepted definitions. The first is more "physical" because facts, data, and instructions can be "collected," where the second definition speaks to the fact that information doesn't exist unless a human assigns a meaning to it. This may be splitting hairs, but think of this. An object like a computer chip is placed in front of two people, one is from the mountains of Tibet and the other from Germany. Assuming the person from Tibet has never seen a chip before, he would assign a different meaning to the object than "computer chip." Assuming the German has seen one before, he would recognize it and define it as a chip. Both would have the right "information" in their own context. Information is the facts, data, and instructions, but more importantly it is also how a human views, associates, and categorizes an object or experience to provide meaning.

Information: 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Publication 1-02)

Figure 3. Definition of Information

People and organizations in the modern world are inundated with thousands of bits and pieces of information a day. They have to look at each one, give it meaning, and then apply mental processes to compare, contrast, and validate the information and act upon it. For example, you read in the newspaper that Sears is having a tire sale. You immediately think: 1) do I need tires? 2) if yes, where did I buy my last set? 3) do I trust Sears? 4) do others have better deals?…you get the idea. This multi-step analysis of information is similar to the processes the military uses to cull intelligence from information (see Figure 4). It is important to remember the difference between information and intelligence.

Intelligence: 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Publication 1-02)

Figure 4. Definition of Intelligence.

Unfortunately the differences aren't always appreciated or understood, especially by the military operational community. Intelligence strives for accuracy while many sources of information are more focused on timeliness. News organizations like the Cable News Network (CNN) have expanded their reach into the crevices of the world to such a degree that almost any event can be globally transmitted within 15 minutes of its occurrence. This far exceeds the military's ability to gather and process information into intelligence. And this gap will never close because the military will never have perfect

intelligence sources to verify data as it occurs. And the cost of error is very low for news organizations because they can retract a story or breaking headline, unlike a country that many not be able to recall or disable a missile or a bomb once it has been launched.

The next level of the information pyramid is knowledge. Knowledge is derived from information that has been tested and accepted as factual. This is accomplished through cognition where unverified information is received, mentally assessed and tested using perception, reasoning, or intuition before the information is accepted as fact. Commanders must ensure that they are dealing with facts and not just their beliefs. Once they have the facts, they can gain an understanding of the situation by using their judgment to put their newfound knowledge into context. “Ideally, understanding a situation supports a commander in battlefield visualization and creates the conditions from which plans can be formed and effective actions taken” (U.S. Army Field Manual (FM) 100-6, 1996, p.2-1).

The importance of understanding to military operations has been widely discussed by classic military strategists. Clausewitz was skeptical of the value of “knowing” in battle because he felt intelligence was often contradictory, its accuracy was questionable , and it just added “friction” (Clausewitz, 1832/1873). But Sun Tzu and Jomini on the other hand, felt good intelligence about an enemy’s plans greatly enhanced the chance for success in battle, all other things being equal. But, the more an enemy understands about your previous plans, existing forces, history, operational doctrine, cultural biases, etc., the easier it will be for him to anticipate or counter your operations. So the goal is to find out as much information about your opponent while preventing him gathering information about you.

2. What are Information Operations?

Information operations are defined as the “actions taken to affect adversary information and information systems while defending one’s own information and information systems” (JP 1-02, p. 211). But the expanded definition presented in FM 100-6, Information Operations, better explains the intent of military information operations:

> Information operations integrate all aspects of information to accomplish the full potential for enhancing the conduct of military operations. Information operations are not new. In their simplest form they are the activities that gain information and knowledge and improve friendly execution of operations while denying an adversary similar capabilities by whatever possible means. (1996, p. iv)

Additionally, there is some confusion in current literature on IO over the relationship between information operations and information warfare. According to current Joint doctrine, Information warfare (IW) is a subset of IO, not vice versa. IW is limited to times of crisis or conflict to achieve a specific objective against a specific target (JP 1-02, p. 211) using primarily offensive IO capabilities. As we will discuss later, IO describes the larger picture and embraces both defensive and offensive capabilities.

3. Why are Information Operations used?

Information operations contribute to the integration of the military element of national power with the other elements to achieve national objectives. The 17 IO capabilities and related activities (see Figure 5) can support U.S. strategic engagement policy throughout the range of military operations (JP 3-13, p. I-10). The effectiveness of deterrence, power projection, and other strategic concepts is greatly affected by the ability of the United States to influence the perceptions and decision making of others. In times of crisis, IO can help deter adversaries from initiating actions detrimental to the interests of the United States or its allies and/or coalition partners. Consider the effectiveness and the "message sent" to the Chinese when the U.S. sent 12 ships including two aircraft carriers to the Taiwan Straits during a Chinese military exercise in 1996. This event of gunboat diplomacy sent both China and Taiwan a message: "to China…don't overplay your hand [and] for Taiwan…The U.S. will back you -- to a point" (McIntyre, 1996).

If carefully conceived, coordinated, and executed, IO can make an important contribution to defusing crises; reducing periods of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in a combat situation. Thus IO, at both the national-strategic and theater-strategic levels, requires close coordination among numerous elements of the U.S. government, to include the Department of Defense.

Electronic Warfare	Operations Security
Computer Network Attack	Civil Affairs
Information Security	Public Affairs
Counter-Deception	Physical Security
Communications Security	Counter-Intelligence
Deception	Computer Security
Physical Attack/Destruction	Counter-Propaganda
Network Management	Computer Network Exploitation
Special Information Operations	

Figure 5. Information Operations Capabilities and Related Activities. From Joint Publication 3-13, Information Operations, October 9, 1998, p. 1-10.

4. Why a National Information Strategy?

Conflict in the infosphere is a series of actions to win the "battle of the story" and affect how the world perceives an event. The "battle of the story" involves more than how the event is portrayed or "spun" by the participants. It involves all of the motivational, emotional, and political methods used by a country, a representative group, or even an individual to present their perspective and to justify their actions in a given situation to the world at large. The battle can take place in any information medium from the Internet to coffee house discussions and college campus rallies to CNN investigative reports. The U.S. historically responds cautiously to any event using public affairs releases and press conferences, presenting only evidentiary information about an event; and if offensive information operations are required, the U.S. will engage in the computer network operations (CNO) of attack and exploitation.

Public affairs (PA) and CNO may be applicable during the initial stages of a conflict, but they don't represent all the information operation tools the U.S. could use in a situation. There are many other IO tools available to assist the U.S. as a crisis or situation develops, but they are frequently overlooked. There is no familiar model or comprehensive plan of how to use all of the IO tools in a response to an event. Both of these shortfalls could be addressed with a national information strategy.

A national information strategy would outline how the U.S. government and all of its agencies and departments react to event and identify what information capabilities could be mobilized. It would provide direction to the proactive planning of IO and provide guidance when responding to a crisis. The national strategy would have to be

flexible, scalable and adaptable to address different situations. At its core, the strategy should consider: 1) the message to be passed, 2) the intended audience, 3) the unintended audience, 4) how to pass the message, and 5) how to prevent an opponent from doing the same with their message.

The foundation of the information strategy is the message. A single, coordinated message to the world builds credibility internationally because the position of the United States on a particular issue has been made clear by all of its agencies. It can be embarrassing to a nation when an important message is clouded by misperceptions. A recent example occurred when President Bush spoke on how dedicated the United States was going to be in the pursuit of international terrorists; he "described America's war on terrorism as a 'crusade,' a term that has an extremely negative historical connotation throughout the Islamic world" (Carpenter, 2001). The term crusade represents a period of 195 years of war with "alien intruders who were bent on senseless destruction" (Haddah, 1993). Muslim historians see "the crusaders as courageous but unrestrained and often treacherous warriors. They find support for this conclusion in such acts as the reckless murder of the civilians, the capture of Muslim women and children, the confiscation of property, and--most symbolic of all--the conversion of Muslim mosques into churches" (Haddah, 1993). From this perspective, it is easy to understand why the Muslim world responded so vehemently when the President of the greatest western power used the term.

This error in perception management vividly demonstrates the importance of identifying and crafting a message considering both the intended and unintended audiences. Although the President's speech was meant to reassure, his "reference to a 'crusade' against terrorism, which passed almost unnoticed by Americans, rang alarm bells in Europe. It raised fears that the terrorist attacks could spark a 'clash of civilizations' between Christians and Muslims, sowing fresh winds of hatred and mistrust" (Ford, 2001). The intended audience understood what the President was trying to say, but the rest of the world received quite a different message. To recover from this misstep, the President and many European leaders spent most of the following days to reassuring the worldwide Muslim community (Ford, 2001).

The negative reaction to America's "crusade" could have been avoided if policymakers had taken the time to determine who was going to listen to the message and crafted it differently (i.e., eschewed the notion of "crusading"). U.S. policymakers must consider all of the countries, organizations, groups and people who have an interest in the issue at hand and how they may react. While it would be impossible for policy makers to consider every last person, it is possible to identify groups of people at a macro level. This would simplify the analysis, but at a risk. If the groupings are too large and represent too many different types of people, the analysis may fail to show the subtle effects of specific information tools. With the risk of oversimplification in mind, the community interested in the war on terrorism was broken into six groups for this analysis: the terrorists (currently al Qaeda), the Taliban, the Afghan population, other Islamic states, the non-allied world, allies of the U.S., and the U.S. population. While it may not be possible to craft a message that pleases all these audiences, an understanding of or an estimated reaction to the message should prevent strategic information gaffes.

Identifying the message, both the intended and unintended audiences, and the means to transmit the message are only the first half of a complete strategy. The second half is figuring out how to use all the available IO tools (see Figure 5). This would prevent an opponent from fully executing their information strategy while allowing the U.S. to execute its own information strategy and protect its IO infrastructure. Or more simply, how the U.S. could achieve information superiority.

D. STRUCTURE OF THE STUDY

Now with a basic understanding of information operations and its key concepts, we will focus on a few additional concepts that are critical in our examination of the benefits of a national information strategy: how IO can be used, how it can be planned, and how it has been used in recent conflicts. Chapter II addresses the first question, how IO can be used. It defines each of the 17 IO elements, discusses the potential synergy in multi-element campaigns, and applies the elements to various levels of war. Chapter III offers a methodology for planning information operations and outlines the linkages to strategic, operational, and tactical objectives. Chapter IV attempts to validate the planning methodology and its associated linkages by evaluating America's response to the attacks on September 11, 2001 and the resulting war on terrorism. How the world's

remaining superpower reacted to al Qaeda, a non-state actor, may provide some interesting insights into the limitations and opportunities of asymmetric of information operations.

Finally, Chapter V summarizes the concepts of information operations and suggests an answer to the question of whether a national information operations strategy would be beneficial to the conduct of military information operations or not. Further, it proposes a conceptual methodology for developing a national information strategy and closes by proposing a number of questions for further research toward this goal.

II. HOW ARE INFORMATION OPERATIONS USED?

We must first understand what information operations are and where they fit in military theory to determine how best to use them. One of the most confusing concepts is the use of the term "information operations." Is it a single entity or a general category of military activity, like "naval operations"? According to current joint doctrine, it is the latter. Information operations are a group of 17 capabilities (see Fig. 6) that allow a commander to meet the requirements of protecting his own information and information systems while affecting an adversary's information and information systems (JP 3-13, p. I-10). Each capability is targeted to a specific area of the infosphere and has unique benefits and associated risks.

Electronic Warfare	Operations Security
Computer Network Attack	Civil Affairs
Information Security	Public Affairs
Counter-Deception	Physical Security
Communications Security	Counter-Intelligence
Deception	Computer Security
Physical Attack/Destruction	Counter-Propaganda
Network Management	Computer Network Exploitation
Special Information Operations	

Figure 6. Information Operations Capabilities and Related Activities. From Joint Publication 3-13, Information Operations, October 9, 1998, p. I-10.

In this chapter, we will discuss how the capabilities relate to each other, and what area of the infosphere each IO capability targets or defends. The chapter will conclude with an analytical concept of information operations as a whole and how it applies to the three levels of war.

A. INFORMATION OPERATIONS AS A SUM OF ITS ELEMENTS

Current joint doctrine splits information operations into two general areas, defensive and offensive information operations. Defensive information operations (DIO) are the information capabilities used to protect your own information and information systems, while offensive information operations (OIO) are the actions that attack or

exploit an adversary's information or information systems. Dividing capabilities into these two categories seems a sound approach. However these categories are limited, because they do not provide enough granularity for decision makers to select specific IO capabilities to use for a type of target.

Using a concept analogous to a computer's hardware and software components, Arquilla suggests DIO and OIO be broken down into those capabilities that affect information technology (hardware) and those that affect how people use their brain, or "wetware," to collect, sort, process, and act on information (software) (2001). We will label these four new subcategories of information operations as information assurance (DIO versus technology), "wetware" standardization (DIO versus mental processes), denial/disruption/destruction operations (OIO versus technology), and perception management (OIO versus mental processes). This new categorizing scheme, shown in Figure 7, should provide a sufficient level of granularity for our purposes.

	Defensive IO	**Offensive IO**
Technology "Hardware"	Information Assurance	Deny/Disrupt/ Destroy
Mental Processes "Wetware"	Wetware Standardization	Perception Management

Figure 7. Initial IO Matrix. From seminar on "Conflict in the Information Age", by John Arquilla, March 2001.

During the course of this analysis, we may find some of the 17 IO capabilities overlap the four new categories. This highlights the duality of some of the IO capabilities and the need for an analytical approach that identifies the overlaps. We will start by looking at the defensive IO categories and then move on to the offensive ones.

1. Information Assurance

The first defensive quadrant contains the capabilities used to protect your own information and information systems, commonly known as Information Assurance (IA) (see Figure 8). IA is defined as "information operations (IO) that protect and defend information and information systems (IS) by ensuring their availability, integrity,

authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (U.S. Government Services Administration, 1996).

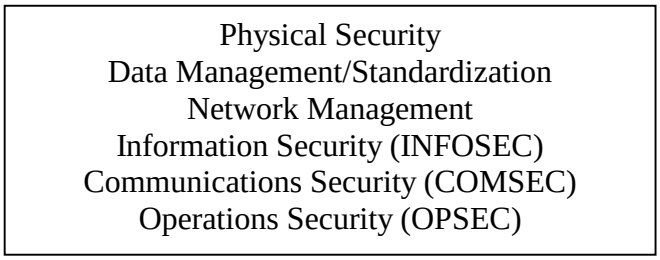

Figure 8. Elements of Information Assurance (DIO vs. technology).

The first capability in IA is physical security. IA is simply the protection of information processing equipment, data, and facilities used to process information. One of the best ways to protect systems is to limit physical access to a computer, a router, or network link (CISCO, 2001). Access controls become more complex and redundant as the sensitivity of the information processed increases. They can start out simple, like locking classified hard drives in a safe, and move to the extreme, like working in a sealed environment with guards and biometric identification systems.

The next IA capability is data management and standardization. Data management is "the control of data handling operations--such as acquisition, analysis, translation, coding, storage, retrieval, and distribution of data--but not necessarily the generation and use of data" (U.S. Government Services Administration, 1996). To make this easier and more efficient, the data should be standardized across the organization to allow the free flow of data.

The third IA capability, network management, is the linchpin of any network. The International Standards Organization Network Management Model outlines the functions of configuration, accounting, fault, performance, and security management. Each is important to an efficient network, but the most important functions to IA and the defense of the network from attack are security and configuration management.

Security management defends the network by controlling access through operating system permissions "so the network cannot be sabotaged (intentionally or

unintentionally) and sensitive information cannot be accessed by those without appropriate authorization" (CISOC, 2002). Configuration management is the second layer of computer network defense (CND). All network software must be continuously updated with the newest security patches or be replaced with newer versions across the network. This will make compromising a network through software or operating system faults significantly harder.

The next two capabilities, information security and communications security, deal directly the procedures concerning data manipulation, storage, printing, filing and the access control procedures required of personnel who have access to data or use the network (e.g., passwords). Communications security also focuses on ensuring secure communications by using special cryptography equipment and keys, limiting access to both.

The last IA capability is operations security (OPSEC). OPSEC is ensuring operational data or plans aren't conveyed to an adversary. Operational information can come from many sources to include monitored phone calls, abnormal activity in organizational buildings at odd hours, spouses mentioning members are going out of town for a period of time while in the store, or many people buying the same kind of supplies from local stores all at once. All are telltale signs that something is going to happen. For example, pizza delivery people in Washington DC can usually tell when the Department of Defense is planning something because the number of pizzas delivered to the Pentagon skyrockets ("And Bomb", 1990).

In general, IA focuses on the technology, but it is dependent on people. It relies on the ability of individuals to think about the situation and take the actions necessary to maintain information security at different levels. This in turn leads organizations to establish standards of behavior and standard operating procedures.

2. Wetware Standardization

The key concept of this quadrant is to understand how an organization manages its own information and information systems through standard operating procedures. As an organization matures and learns to survive in its environment, it establishes standard procedures and accepted practices based on experience. This institutional knowledge is

passed along to all of the organization's members through the capabilities listed in Figure 9. The conformance mandate starts when a new employee is indoctrinated into the organization. He or she is taught how the organization is structured and the "chain of command", how to function in the organization, and respond in organizationally appropriate ways to situations. This "programming" of an individual's wetware is intended to standardize how people in the organization function at all levels to maximize efficiency.

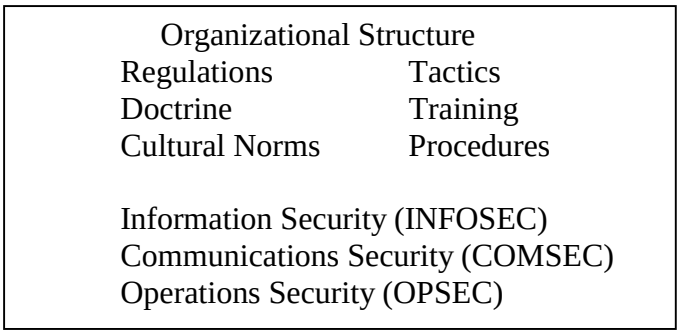

Figure 9. Elements of Wetware (DIO vs. mental processes).

The standard operating procedures associated with INFOSEC, OPSEC, and COMSEC are all anchored in an individual's thought processes. All security programs rely on the mental ability of the individual to understand the policies and always " do the right thing." They must realize the ramifications of their actions, from discussing operational information on an open telephone line to sending people's social security numbers over unclassified email.

3. Denial/ Disruption/Destruction Operations

Denial/Disruption/Destruction operations involve attacking an adversary's information infrastructure directly using both kinetic and electronic capabilities. This quadrant represents the IO capabilities usually first thought of and most frequently used because they are the hard, physical, hands-on capabilities of IO (see Figure 10). Most decision makers like the straightforwardness of the denial/disruption/destruction capabilities because they represent the "force on force" military model of normal physical warfare.

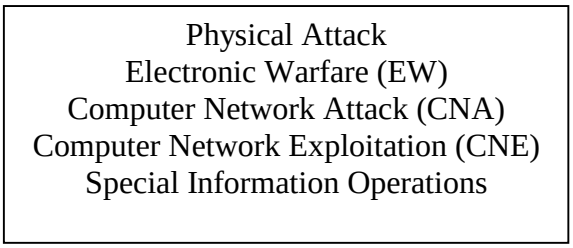

Figure 10. Elements of Denial/Disruption/Destruction Operations (OIO vs. technology).

Each of the capabilities in this quadrant of our matrix can be used to deny, disrupt, or destroy an adversary's information or information infrastructure. The level of attack could only be assigned after a thorough target analysis to determine the level of damage to attain the desired information objectives. For example, a physical attack could damage or destroy a communications tower, radio antenna, or a command and control bunker. Additionally, the electronic warfare capabilities could use electromagnetic energy to interfere with broadcasts and communications or EW could use directed energy to destroy enemy information infrastructures or deployed forces.

Offensive computer network operations (CNO) are broken down into two subcategories: computer network attack (CNA) and computer network exploitation (CNE). CNA involves breaking or "hacking" into an opponents information system and either destroying it or rendering its data unusable. While CNE involves monitoring the activity on a system, placing fictitious data in the system to confuse the enemy, or any other activity that comes short of destroying the opponent's system or its data. The goal of exploitation is to gain as much information as possible from your adversary or place as much fictitious data as possible without them knowing you are doing it.

The last capability is special information operations (SIO). The only published definition or description of an SIO is found in Joint Publication 1-02. It is purposely vague and only discusses the reason for a special approval process. It can be reasonably assumed that SIO are related to special activities. They are missions

> conducted in support of national foreign policy objectives that are planned and executed so that the role of the US Government is not apparent or acknowledged publicly. They are also functions in support of such activities but are not intended to influence US political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions (Joint Publication (JP) 1-02, p. 403)

4. Perception Management

The last quadrant in our matrix is perception management. It is comprised of the IO capabilities that are used to affect the information an adversary uses to make decisions. It wages the "battle of the story" in the court of world opinion (see Fig. 11). JP 1-02 defines perception management as the

> actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. (p. 332)

Public Affairs (PA)	Deception
Counter-deception	Electronic Warfare (EW)
Counter-propaganda	PSYOP
Counter-intelligence	Special Information Operations
Counter-PSYOP	

Figure 11. Elements of Perception Management (OIO vs. mental processes)

The first capability is public affairs (PA). Its core mission "is to expedite the flow of accurate and timely information about the activities of US joint forces to the public and internal audience" (JP 3-61, p I-1). Entire theses have been written on the relationship between the military and the media. We will accept the relationship as described in current joint doctrine. In this study, we are more interested in the requirement for the PA, civil affairs (CA), and psychological operations (PSYOP) messages to be coordinated. Message deconfliction is crucial because the PA, CA, and PSYOP messages must not contradict one another or the credibility of all three will be lost because information overlaps audiences. To prevent overlap, contradiction, or

compromise of deception plans, PA needs to be involved early in the operational planning process and throughout the operational campaign (JP 3-61, pp. III-12-13).

The next set of perception management capabilities we will discuss are the family of countering operations: counterdeception, counterpropaganda, counterintelligence, and counterpsychological. By expanding the Joint Publication 1-02 definition of counterdeception, we will define countering operations as "activities to negate, neutralize, diminish the effects of, or gain advantage from foreign perception management operations…[but they do] not include the intelligence function of identifying foreign perception management operations" (p. 104). They allow a commander to offer a different message to counter an adversary's perception management messages.

Now we will discuss deception. The U.S. military engages only in military deception because current DOD policy forbids the targeting or misleading of the U.S. public, the U.S. Congress, or the U.S. news media. The military may "deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission"(JP 3-58, p. I-4). A critical part of the deception planning process is to coordinate the program with the PA officers to "reduce the chance that public affairs officers will inadvertently reveal information that could undermine ongoing or planned deception operations" (JP 3-58, p. I-4).

In addition to its deny/disrupt/destroy roles, Electronic warfare (EW) can be used subtly to limit the ability of an adversary to collect accurate intelligence, or use the electronic spectrum to broadcast or transmit their message. Friendly forces can use electronic masking to conceal an operation or present a false situational picture by transmitting controlled electromagnetic energy on friendly frequencies while protecting friendly transmissions and systems. Electronic masking presents false or ambiguous data to adversary SIGINT or electronic surveillance efforts through disguising, distorting, or manipulating friendly sensor data (JP 3-51, p. III-5).

EW also enables other perception management capabilities, especially deception and psychological operations. An example of EW supporting PSYOP is the jamming of

radio and television broadcast signals so that friendly programming can be transmitted. Like all the other perception management capabilities, the effectiveness of EW is dependent on deconfliction and coordination.

5. Understanding The Whole IO Picture

By compiling the four IO categories into a single matrix (see Fig. 12), the integrated nature of IO becomes apparent. The need to consider the whole range of IO capabilities and not focus on a single IO category when developing operational plans becomes apparent. The matrix provides a powerful analytical tool to guide the development of information strategies and plans. It is also possible to use the matrix to critically evaluate past or ongoing information operations campaigns, which we will do later in this study.

	Protect Own	**Affect Others**
Technology "Hardware"	**Information Assurance** Physical Security Data Management/Standardization Network Management Information Security (INFOSEC) Communications Security (COMSEC) Operations Security (OPSEC)	**Deny/Disrupt/Destroy Ops** Physical Attack Electronic Warfare (EW) Computer Network Attack (CNA) Computer Network Exploitation (CNE) Special Information Operations
Mental Processes "Wetware"	**Wetware Standardization** Organizational Structure Regulations Tactics Doctrine Training Cultural Norms Procedures Information Security (INFOSEC) Communications Security (COMSEC) Operations Security (OPSEC)	**Perception Management** Public Affairs (PA) Counter-propaganda Electronic Warfare (EW) Counter-intelligence PSYOP/Counter-PSYOP Deception/Counter-deception Special Information Operations

Figure 12. The Information Operations Matrix. From unpublished notes from a series of seminars on "Conflict in the Information Age", by John Arquilla, March 2001.

B. IO IN WAR

Now that we know how and why IO is a sum of its capabilities, we need to determine how to actually apply IO in war. It may sound like a simple task, but it's not because information operations are a unique set of capabilities that can cut across all the

levels of war: strategic, operational, and tactical. We will discuss how IO could be used in each level of war, apply a selection of IO capabilities, and describe the potential result.

1. IO and the Strategic Level of War

At the strategic level of war, IO may be used to achieve national objectives and influence or affect an adversary's national power elements (political, military, economic, or informational), while protecting similar friendly elements. Using IO at this level requires a high degree of coordination among all the participating agencies in the U.S. Government (USG), allies, and coalition partners to be successful (U.S. Air Force Doctrine Document (AFDD) 2-5, p.28).

Examples of strategic information operations include using public affairs and counterpropaganda operations to "create a lack of confidence in an adversary's military, diplomatic, or economic ability to achieve its goals or defeat US goals" (AFDD 2-5, p. 29) in a crisis or conflict. Another is using computer network exploitation and electronic warfare to "incapacitate an adversary's ability to lead due to lack of communication with its forces or understanding of the operating environment" (AFDD 2-5, p.29).

2. IO and the Operational Level of War.

Operational-level IO supports campaign and major operation objectives by targeting an adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities while protecting friendly ones. This will limit how much information an adversary can gather and use, and thereby limit his situational awareness, ability to effectively command and control his forces, and sustain his logistical tail, which should give friendly forces a significant advantage.

Examples of operational information operations include using electronic warfare, computer network attack/exploitation, physical attack to render an adversary's automated command and control systems useless by disrupting the network infrastructure; implanting bad or misleading data and "fogging up" his situational picture; or causing the sudden loss of critical network nodes and connections to power supplies. Any and all of these would reduce the operational tempo of the adversary and his ability to amass forces. Another example is psychological and electronic warfare operations using leaflets,

radio/television transmissions, psychological bombing (e.g., BLU-82s) to entice adversary troops to surrender or desert.

3. IO and the Tactical Level of War

Tactical-level IO focuses on denying adversary units the use of their information and information systems for command and control, intelligence, and other combat related functions. This is accomplished by using as many of the OIO capabilities as possible and not just limiting actions to those found in deny/disrupt/destroy quadrant of the matrix.

Examples of tactical-level IO include using PSYOP speaker teams with linguists or leaflet artillery shells to entice the adversary to surrender, and the use of local area radio jammers (electronic warfare) to jam the adversary's transmissions.

C. CONCLUSION

In this chapter we examined information operations capabilities by first categorizing them and then looking at each one individually and discussing its potential uses. We started by accepting the division of the 17 IO capabilities into two major categories, defensive and offensive information operations. But we pointed out that this didn't provide a convenient framework for commanders to evaluate their information operations alternatives. We suggested dividing the two major categories again by separating the capabilities by their targets, hardware and mental processes. This created the four new categories of information assurance, wetware standardization, deny/disrupt/destroy operations, and perception management.

We then reviewed the capabilities within the new categories and presented examples of how each could be used. The four new categories were then compiled into a matrix that we suggested could be used as an analytical tool for commanders. It could match an IO capability (DIO or OIO) to a type of target (hardware or wetware). We closed the chapter by looking at how IO could be used in each level of war and some examples.

Next we will develop a methodology for planning information operations and for integrating them into overall theater campaign and operational plans.

THIS PAGE INTENTIONALLY LEFT BLANK.

III. HOW SHOULD IO BE IMPLEMENTED?

Now that we have a basic understanding of information operations capabilities, we must determine how and when to use them. Joint doctrine offers specific methods for planning both defensive and offensive information operations capabilities. The Joint Publications look at the planning process from the unique point of view of each IO capability (e.g., PSYOP, Electronic Warfare). While this approach is very useful for operational and tactical IO planning, it may prove insufficient to develop strategic level IO plans and policy.

A strategic level planning method must provide direction to all organizations that participate in information operations so the synergy of an integrated IO campaign can be achieved across the government. Current doctrine does not provide a planning methodology for strategic or national level information operations. The business sector may provide an example we can adapt to meet the requirements of planning for information operations.

A. NATIONAL STRATEGIC DIRECTION

All military operational plans require clear national strategic guidance and direction to ensure they align with the overarching concepts, doctrine, and goals of the national security policy. The United States has a process to ensure this happens. It is called the National Strategy Direction system. It starts with the President and his National Security Council and ends with a National Military Strategy (NMS) that reflects the nation's economic, diplomatic, military, and informational goals. A short review of how national security direction is distilled into national military strategy (NMS) will provide a foundation before we develop an IO planning methodology.

The National Strategy Direction system (see Figure 13) starts at the top of the Executive Branch with the President of the United States and his National Security Council (NSC). The NSC

is the principal forum for deliberation of national security policy issues requiring [a] Presidential decision. The NSC…develops policy options, considers implications, coordinates operational problems that require interdepartmental consideration, develops recommendations for the President, and monitors policy implementation…The NSC prepares national security guidance that, with Presidential approval, implements national security policy. (Joint Publication 1, p. I-2)

Figure 13. National Strategic Direction. From Joint Publication 3-0, Doctrine for Joint Operations, September 10, 2001, p. I-4.

Once the National Security Strategy (NSS) and other national policy statements have been published, the next step is to develop the National Military Strategy. It "entails the art and science of distributing and applying military power to attain national objectives in peace and war [and] provides the advice of the Chairman of the Joint Chiefs of Staff (CJCS) in consultation with the Joint Chiefs of Staff and the Combatant Commanders on the strategic direction of the Armed Forces over the next three to five years" (Shalikashvili, 1997, p. 3). The two primary documents, the "National Security Strategy and NMS, integrate national and military objectives (ends), national policies and military concepts (ways), and national resources and military forces and supplies (means)" (JP 3-0, p. I-4).

The final document in the process is the Joint Strategic Capabilities Plan (JSCP). It "provides guidance for planning purposes to the combatant commanders and the Chiefs of the Services to accomplish tasks and missions based on current military capabilities" (JP 3-0, p. I-4). Combatant commanders take this information and use it to form their theater or functional strategies and plans to conduct military operations, completing the linkage process of national strategy to operational and tactical military plans (JP 3-0, p. I-5).

One shortfall of the current process is the lack of clear direction for the informational aspect of national power. The current National Security Strategy discusses protecting information infrastructures and preventing asymmetrical information operations but does not specifically outline an informational strategy. We will address this shortfall later.

B. A BUSINESS MODEL?

The government has had mixed success in adapting techniques, models, and philosophies from business (e.g., Total Quality Management). But past problems shouldn't prevent us from adopting successful business-planning concepts and deriving new approaches to planning information operations.

In many ways information is like a consumer product. A product must be formulated, produced, labeled, shipped, stocked, sold, and the sales tracked to determine if the product is meeting the market's demands. Information is very similar. It may be possible to leverage the lessons learned in the business world to more efficiently operate in the infosphere. Many military applications of information operations are similar to commercial fields. For example Public Affairs is similar to the Public Relations and it could be argued that PSYOP is like the Marketing Department of a company, at a very macro level. Each is concerned with altering your perception of a product, may it be an idea or a can of soup. Not all the IO capabilities have business counterparts, but the structure of marketing planning is similar to the planning methodologies described in the Joint Publications for each of the perception management capabilities.

The business analogy may not be as extreme as it may seem. The State Department hired Charlotte Beers, a marketing expert with 40 years of experience, as the

Under Secretary for public diplomacy and public affairs to "refurbish America's image abroad" It was hoped that her marketing expertise would help the United States recast its image in the Middle East. Beers recently said, "we're going to have to communicate the intangible assets of the United States—things like our belief system and our values." She then compared the image of the United States to a brand image in which the goal is to "build a relationship between the product and its user" (Starr, 2001, pp. 56-58).

To build a brand, a company or in this case the nation must market its product to the world. To do this we will look at a marking planning methodology that should highlight some areas to be considered in IO planning. Roman Hiebing and Scott Cooper offer at ten-step marketing planning process (see Table 2), which they claim, will enable the user to "define issues, answer questions correctly, and make decisions"(1996, p. xxvi). They go on to discuss the merits of their approach and some of their comments have applicability to IO planning as well. Here are some excerpts worth noting (Heibing & Cooper, 1996, p. xxviii):

- One needs a well-defined methodology to sort out and interface these many overlapping elements
- Disciplined…planning employs a sequential, step by step system that asks for consideration of all tools and takes the marketing through a clear incremental building process
- The sequence of how the plan is ordered is important because what comes *after* in the order of the plan is, in effect, making what comes *before* possible
- The evaluation step…closes the loop on this continuous and comprehensive planning process.

If you look closely at the descriptions of each step of Heibing and Cooper's approach and disregard the specific business references, it is readily apparent how each could apply to planning for information operations, both technical and against wetware.

Table 2. The ten steps to disciplined marketing planning. From *The Successful Marketing Plan*, Hiebing and Cooper, 1996, pp. xxviii-xxxii.

	Title	Description
Step One	Business Review	Situation analysis of market
Step Two	Problems/Opportunities	Summary of challenges of market
Step Three	Sales Objectives	Projected levels of goods to be sold
Step Four	Target Markets and Marketing Objectives	Define target group/target behavior desired
Step Five	Plan Strategies	Positioning strategy for the image of your product and strategies to fulfill objectives
Step Six	Communication Goals	Set target market awareness and attitudes to deliver positioning and fulfill marketing objectives
Step Seven	Tactical Marketing Mix Tools	Marketing executions to fulfill objectives and plans above. Each tool should have its own objectives, strategies, and executional specifics
Step Eight	Marketing Plan Budget & Calendar, Payback analysis	Cost, timeline, and anticipated net receipts of marketing plan
Step Nine	Execution	Execute the plan, hope the target market buys product
Step Ten	Evaluation	Determines level of success in marketplace and relates changes needed to next iteration of marketing plan.

C. IO PLANNING PROCESS

Heibing and Cooper's method provides a deliberative planning template for the new information operations planning methodology we will use (see Table 3). It ensures that a decision maker develops a comprehensive IO plan that supports national strategy. It is also broad enough to address the entire range of information operations. But, to fully understand how to use this new approach, we will discuss each new step individually.

1. Review Strategic Environment

This is the most critical step in our process because it is where the U.S. evaluates the situation, determines where it sits in the world order, where it wants to be in that order, and how can the situation be changed if need be. This process truly builds the IO foundation for future operations.

Table 3. An IO planning methodology.

	Title	Description
Step One	Review Strategic Environment	Situation analysis guided by national strategy
Step Two	Identify Problems/Opportunities	Summary of challenges/opportunities to overcome/exploit
Step Three	Establish Informational Objectives	What an informational campaign should achieve
Step Four	Target Technology or Audiences	Define target group/target behavior desired
Step Five	Develop Theme or Message	Positioning strategy for to match the theme or message to the target audience
Step Six	Establish IO Goals	Set target market awareness and attitudes to deliver positioning and fulfill marketing objectives
Step Seven	Chose IO Capabilities Mix	IO executions to fulfill objectives and plans above. Each capability should have its own objectives, strategies, and executional specifics
Step Eight	Complete Risk/Benefit Assessment	Review relative cost, time, and risk compared to net results of IO plan
Step Nine	Execute and Monitor IO	Execute the plan, hope the target technology or audience is affected. Gather data during execution for evaluation.
Step Ten	Evaluate and Modify	Determines level of success and apply needed changes to IO plan

2. Identify Problems/Opportunities

This step takes the results from the review and tries to identify any problems with the messages or ideas the United States wants out in the infosphere. We can also identify any opportunities where we can exploit a situation to provide a counter message or correction to erroneous information about the United States in the infosphere.

3. Establish IO Objectives

Armed with potential problem areas and opportunities, it is possible to develop a plan and derive objectives to attain using information operations. Information operations objectives should be broad enough at the strategic level to grant wide latitude in meeting them. But they should also be descriptive enough to ensure the proper actions are taken to

meet the national strategic goals. The IO objectives are will drive the rest of the planning process and will be the criteria to evaluate the missions once complete.

4. Target Technology or Audience

The next step is to take the objectives and determine who or what should be targeted for the particular information operation. In many cases, both technology and wetware will be targeted to affect both the adversary's ability to use his equipment and to make knowledgeable decisions. This step requires detailed intelligence on the potential targets to be successful.

An important point to make here is not to forget to look at all the technologies and audiences that are "connected" to your target or in your ability to launch an IO. Collateral damage to alliances, international relationships, friendly information infrastructure, coalition forces, public support at home, and international perceptions can negate the results of an otherwise successful IO.

5. Develop Theme or Message

This step may involve two subprocesses. For the technology targets, a theme may provide a touchstone or motivating idea for those supporting the IO, like "Remember 9/11." If the target is an audience, a message and/or a theme will have to be created that will entice the target audience to modify their behavior or concept of the issue in line with the IO objectives. It is important to consider the "message content, tone, communication vehicle, and frequency" (Heibing & Cooper, 1996, p. 380) when targeting internal and external audiences.

6. Establish coordinated IO Goals

The next step is to use the foundation of information built in the previous steps and align the entire operation with the other elements of national power by establishing goals for the IO. This will allow the IO to support the objectives of the other elements and vice versa. Unlike objectives, which are prescriptive, these goals should be descriptive of the actions needed to affect the target's behavior (Heibing & Cooper, 1996, p. 204). In this step we use these goals to divide the task at hand so the appropriate IO capabilities can be assigned to each subtask. This is a complex process because the

environment is constantly changing, and what was once a valid IO goal could easily be overcome by events.

7. Choose IO Capabilities Mix

With a set of IO goals, the next step is to assign those IO capabilities most applicable to accomplishing each goal. This can be a straightforward process, but it can also involve assigning IO capabilities in an oblique manner to achieve an IO goal. Creativity and imagination is often the key to IO success. Remember the Chinese use of a simple computer-generated MPEG file of the fighter and EP-3 mentioned in Chapter 1. It is easy to imagine their IO goal was to tilt world opinion in their favor. They achieved this to a degree by blending Public Affairs, PSYOP, and deception.

An important concept to consider while formulating the IO capability mix is that the IO capabilities, especially the perception management capabilities, are not "off or on" capabilities. They can be targeted to specific subaudiences and used in degrees of aggressiveness.

8. Complete Risk/Benefit Assessment

The last step before execution is to complete an objective assessment of the cost, time and risks versus the end benefit of the plan as it currently stands. Objectivity is the key here. No plan is going to be perfect, but a good plan should be free of critical defects. If critical problems or shortfalls are identified, then return to the step that addresses the problem area and restart the planning process from there. If the plan has no critical shortfalls and the risks in cost and time are acceptable, then the next step is to execute the plan.

9. Execute and Monitor IO

Good execution is the key to success of any plan, especially IO. The IO plan is greater than the sum of its elements, as the effect of each element is enhanced by the impact of the other elements. Attention to detail "assure[s] that the synergistic effect of all the…[IO] plan activities will take place" (Heibing & Cooper, 1996, p. 374).

As the plan is executed, it should be monitored for compliance with the IO objectives and goals. Any deviations in execution or result should be noted and used to evaluate the plan.

10. Evaluate and Modify

Finally, all efforts require continuous monitoring to gauge the effectiveness of the IO campaign. The IO objectives and goals are the scorecard for the campaign. This evaluation process is not limited to an after action analysis, it should be ongoing during the execution of an IO campaign so that timely changes can be made within the dynamic environment of the infosphere and realpolitik.

D. DELIBERATE AND CRISIS IO PLANNING

Information flows around the world all the time and the United States must be prepared to respond in an instant. The continual evolution and revolution in information technology is collapsing the infosphere to a point where almost everyone will only have one degree of separation from everyone else. This near point-to-point connectivity will dictate rapid informational responses to world events.

There will still be a need to do deliberative IO planning in support of theater operational and tactical operations. But these plans will have to be reviewed more frequently to keep up with emerging technology and the ever-changing situation in the infosphere. The planning method presented would be especially useful in a crisis because it logically guides the planner through all the required areas so nothing is overlooked during the heat of the battle.

E. CONCLUSION

In this chapter we looked at how National Strategic Direction currently guides the development of the National Military Strategy. And we found the current Joint doctrine to be focused only on the operational and tactical level of IO, so a new strategic IO planning methodology is needed to assist decision makers. The business world offers some ready templates for organizational approaches to strategic thinking. One is the concept of a marketing plan.

We took the basic marketing plan and modified the ten steps to provide a linear process to ensure all the aspects of IO are addressed during the planning process. After discussing each step, we concluded the chapter with a discussion of how the near point-to-point connectivity in the infosphere makes planning for IO a continuous activity.

Next we will use the IO planning methodology to evaluate the U.S. response to the terrorist attacks on September 11, 2001 and during the first few months of the war on terrorism.

IV. IO IN THE WAKE OF 9/11

The American government's reaction to the terrorist attacks of September 11, 2001 provides a timely glimpse into how the government plans and executes the informational aspects of national power during a time of crisis. Through the chaos created by the attacks on the World Trade Center and the Pentagon, the Administration had to respond quickly to the situation by providing the nation with information and direction. This analysis will use the IO planning methodology developed in the previous chapter to evaluate the informational response of the United States to terrorist attacks.

Many of the details of exactly what the Administration did during the period immediately after the attacks have not been made public. It is reasonable to assume the Administration followed a logical crisis response process similar to our IO planning methodology. We will compare what information is available on the events shortly after the attacks to the IO planning methodology.

Immediately after the second plane hit the World Trade Center and the third plane hit the Pentagon, the President and his advisors took actions that fit the logic of steps one through four of the IO planning method. First, they analyzed the strategic environment and decided to put the government on a high state of alert in case of additional attacks. After things calmed down a little and the initial shock of the attacks wore off, they overcame the challenges and found opportunities to get their messages out. The Administration seemed to have the clear informational goals of: reassuring the country that the government was still in place; all efforts were being made to help those affected; and "the United States [would] hunt down and punish those responsible for these cowardly acts" (Bush, 2001). Additionally, they wanted to reassure the Muslim community that Islam was not under attack by the United States; and any country suspected of supporting terrorism should understand that the U.S. would respond militarily if the supporters didn't change their allegiance.

The Administration tried to relay their message to specific audiences by specifically addressing them in press conferences and speeches. The Administration attempted to send clear signals to the terrorists and the countries supporting them that the

U.S. would bring them to justice. And the Administration also tried to reassure our allies, the Muslim world, and the American people that the terrorists not Muslims were the targets of America's interest and that the U.S. would not rest until the perpetrators were apprehended. This played into the Administration's developing theme of "justified retaliation" ("Bush gets", 2001, ¶ 2). America had been attacked and almost every other country quickly supported the right under international law of the United States to take unilateral retaliatory action against those organizations or states responsible.

With the elements of the first six steps of our IO planning methodology complete, next was to determine the mix of IO capabilities to employ. The selection requires careful thought based on the IO objectives, themes, and goals described above. According to published reports, the U.S. has focused on the offensive information operations (OIO) capabilities of physical attack, electronic warfare, limited psychological operations, computer network exploitation, and computer network attack. Combat operations against the Taliban radio stations and the Al Jazeera television station would support both physical attack and electronic warfare goals to limit the ability of al Qaeda to get its message out (McCaleb, 2001, ¶ 4). Psychological operations have been limited to leaflet drops and aerial radio broadcast providing information about humanitarian assistance and "messages encouraging enemy troops to surrender and give up the fight" (Williams, 2001, ¶ 7). And finally, the recent round up of al Qaeda operatives around the world indicates their networked organization has been compromised potentially through computer network analysis and exploitation capabilities by using traffic analysis programs that trace the routes emails take thru the Internet; and "sniffer" programs that look for certain word combinations within emails (Salkever, 2002, ¶ 3).

If these are the only OIO capabilities used, then the U.S. failed to take full advantage of the capabilities of deception, counterpropaganda, public affairs, civil affairs, counterintelligence, and special information operations. No evidence could be found in unclassified sources that suggested there was national level information direction or centralized information policy to follow in preparing the operations. This became apparent with the early stumbles over the name of the operation, "INFINITE JUSTICE", and the whole debacle over "crusading."

A working group on Special Information Operations, four graduate students, including the author of this thesis, developed an analysis tool to examine how all IO capabilities might be applied to all audiences. The group then spent many hours discussing the nuances of the relationships and potential applicability of each IO capability to each audience. The following is the author's summary of those discussions and conclusions.

A. IO CAPABILITIES MIX ANALYSIS

This analysis examines only the offensive information operations capabilities with the exception of physical attack and special information operations. Both of these are always options but have potential military repercussions. It will be assumed that all of the DIO capabilities were activated at all levels within the U.S. because of the increased information condition (INFOCON) levels right after the terrorist attacks. The level of vigilance to DIO was demonstrated when most all government web sites were shut down immediately after the attack.

The analysis relies on the list of target audiences and technologies, then a subjective assessment of the applicability of each IO capability to and relative effect on each target audience or technology is made. A capability is "applicable" when it affects the target audience or the enabling technology in a measurable way. If applicable, then an estimate of its effectiveness is made using the following grading scale: great effect, some effect, little effect, and no effect. Definitions of each of the ratings are provided in Table 4. The results of the analysis are compiled into a single matrix for each intended audience. We have defined the intended audiences of the war on terrorism as: the terrorists (al Qaeda), the Taliban, the Afghan population, other Islamic states, the non-allied world, the U.S. allies in the war on terrorism, and the U.S. population.

It is worth noting that in some instances, an extremely fine line was drawn between the ratings. When in doubt, a conservative position was adopted rather than chance overestimating the effectiveness of a capability. Also, each assessment was reevaluated to ensure no "mirror imaging" took place that might taint the objectivity of the analysis.

Table 4. Applicability ratings.

***	Great Effect	The tool could eliminate, or fully disrupt (no workarounds possible) the target audience's ability to transmit their message or use their technology.
**	Some Effect	The tool could partially disrupt (workarounds possible), or severely degrade the target audience's ability to transmit their message.
*	Little Effect	The tool could minimally disrupt (nuisance) and minimally degrade the target audience's ability to transmit their message.
-	No Effect	Either the tool had no effect or wasn't applicable to the target audience due to convention, law, or current technological ability.

This matrix approach can be used to look at the IO strategy problem from many different perspectives. While this demonstrates the strength of the matrix method, it can also cause confusion. This analysis focuses only on the applicability and potential effectiveness of the information operations capabilities. A short explanation will be provided for the effectiveness rating assigned to each IO capability for each audience. And then the individual matrices will be compiled into a single color-coded matrix for a final strategic analysis. An example of the color-coded composite matrix is shown in

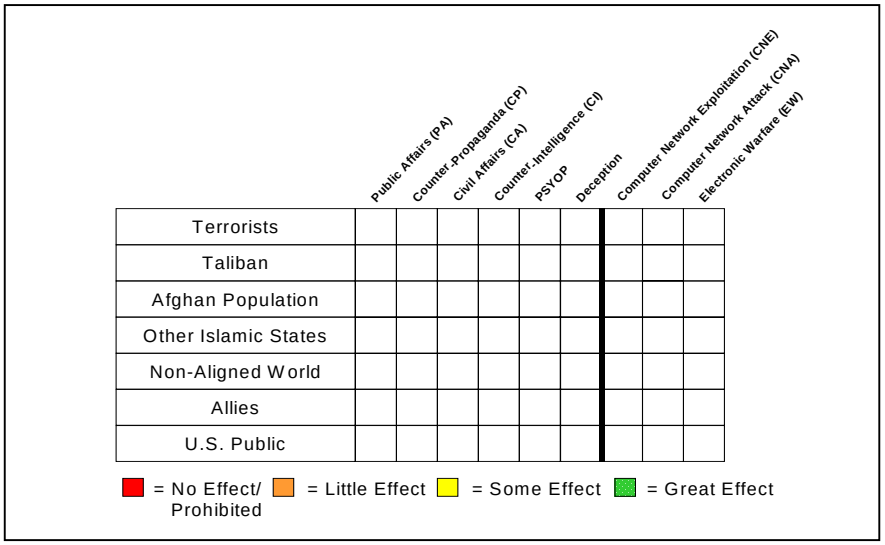

Figure 14. Analysis matrix.

1. Al Qaeda Terrorists

The group is "a coalition of disparate radical Islamic groups of varying nationalities…work[ing] toward common goals – the expulsion of non-Muslim control or influence from Muslim-inhabited lands" (Katzman, 2001, p. 9). Al Qaeda abhors Western influences but happily "rides the rails" of the modern information infrastructure to achieve its extremist goals. Usama bin Laden has been reported using satellite telephones, cellular telephones, computer networks as well as personal messengers to guide the worldwide coalition of terrorist organizations (Sieberg, 2001, p. 1). This unique mix of high and low tech will present a challenge to any IO effort waged against him. Below is an estimate of the effectiveness of the IO capabilities and tools against the al Qaeda terrorists. A summary of the analysis is presented in Figure 15.

- Public Affairs: U.S. efforts to present accurate information would have little effect on terrorists directly.
- Counter-Propaganda: U.S. counter-propaganda efforts would have little effect on hard-core terrorists who are heavily indoctrinated with their organizations' beliefs.
- Civil Affairs: Traditional CA missions would not be applicable directly to the terrorists.
- Counter-Intelligence: Successful CI efforts would have a great effect. Denying them the ability to carry out acts of sabotage and terrorism would deprive them of their main method to gain visibility.
- PSYOP: PSYOP could have great effect on the morale and mental attitudes of terrorists.
- Deception: Deception could have great effect if carried out in a way to inhibit the terrorist's ability to move and act.
- Computer Network Exploitation: CNE could provide some stunning information on the operations of terrorist organizations as long as they rely on computers or larger international networks (like the worldwide web) to move information. The assessment of great effect is predicated on this dependence on larger computer networks to clandestinely move information.
- Computer Network Attack: CNA is rated as having little effect because most terrorist organizations wouldn't risk setting up a standing network in a building or office. It is much easier to use ubiquitous internet cafes and other organizational sites to transmit information to the terrorist organization.

- Electronic Warfare: EW could be of great effectiveness if it is determined what types of communication gear the organization is using and determining how to exploit or deny its use.

Al Qaeda Terrorists	
Public Affairs (PA)	*
Counterpropaganda (CP)	*
Civil Affairs (CA)	-
Counterintelligence (CI)	***
Psychological Ops (PSYOP)	***
Deception	***
Computer Network Exploitation (CNE)	***
Computer Network Attack (CNA)	*
Electronic Warfare (EW)	***
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 15. Applicability of IO against terrorists.

2. The Taliban

Although defeated as of the date of this analysis, this group represented a state sponsor of terrorism and is a good example of a less technically-oriented society that represents a significant number of third world countries. If anything, the Taliban represents an extreme case because they openly pursued a campaign to purge society of almost all advanced technology.

Since the time they gained control over most of Afghanistan territory in 1996, the Taliban pursued an isolationist and fundamentalist Islamic agenda. Their movement represented an ideological mixture of rural Pashtun values, Islamic fundamentalism and totalitarian thinking. Their goal was to establish the world's 'purest' Islamic state, banning what they perceived as corrupting agents and frivolities like television, music and cinema. ("Taliban", 2001)

Because of their disdain for technology and modern technology, an effective IO campaign will be difficult using modern means, but not impossible. The estimate of the applicability of the various IO capabilities against the Taliban follows, and a summary is presented in Figure 16.

- Public Affairs: U.S. efforts to present accurate information would have little effect on the Taliban government itself because they firmly believe in their cause.
- Counter-Propaganda: U.S. counter-propaganda efforts could have great effect on the Taliban's ability to garner support or positive world opinion because the U.S. could come out and refute every allegation. This could cause the Taliban government embarrassment and loss of any prestige it has in the world.
- Civil Affairs: Traditional CA missions would not be applicable directly to the Taliban themselves. Even CA actions taken in Pashtun areas of Afghanistan would not affect the position of the government.
- Counter-Intelligence: CI would have little effect on the Taliban because they are isolated and are focused on themselves with little regard for world opinion.
- PSYOP: PSYOP could have great effect on the morale and mental attitudes of the Taliban if they could be convinced their objectives are unattainable. The challenge will be getting the message to them.
- Deception: Deception could have great effect if carried out in a way to reduce the Taliban's ability to move and act.
- Computer Network Exploitation: CNE would have little effect on the Taliban government. Their abandonment of technology isolates them from this IO tool.
- Computer Network Attack: CNA would have little effect on the Taliban government. Their abandonment of technology isolates them from this IO tool.
- Electronic Warfare: If the information and communications infrastructure of the Taliban were known, EW could be very effective to exploit or deny its use.

3. The Afghan Population

Afghanistan is a country of 26 million people who live in abject poverty under a severe interpretation of Islamic law where the average life expectancy for a man is 46 years and only 45 for women ("Afghanistan: Country Profile", 2001). Twenty-one years of civil war have forced over 500,000 Afghanis into refugee camps in neighboring countries ("Afghanistan", 2001). And six years of Taliban rule has eliminated most of the

Taliban	
Public Affairs (PA)	*
Counterpropaganda (CP)	***
Civil Affairs (CA)	-
Counterintelligence (CI)	**
Psychological Ops (PSYOP)	**
Deception	***
Computer Network Exploitation (CNE)	*
Computer Network Attack (CNA)	*
Electronic Warfare (EW)	***
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 16. Applicability of IO against the Taliban.

information infrastructure in Afghanistan. In 1999 there were only an estimated10 television stations serving only 100,000 television sets, and a single radio station in Kabul serving 167,000 radios ("Afghanistan", 2001). This dispersal of the Afghan people and the elimination of the county's infrastructure will present an extreme challenge to the traditional U.S. use of information operations. It has been widely reported that the general population of Afghanistan is anti-Taliban and there is a desire for a new form of government. This positive environment should enhance the applicability of certain IO capabilities. Below is an assessment of the applicability of IO capabilities and tools towards the Afghan people. A summary is presented in Figure 17.

- Public Affairs: U.S. efforts to present accurate information would have little effect on the people of Afghanistan directly because their lives are not affected by current world events. Some would listen to objective news broadcasts to monitor the conflict with the Taliban via radio.
- Counter-Propaganda: U.S. counter-propaganda efforts would have little effect on the average Afghani. Although clear news and a counterpoint to the Taliban's message could build good will, the lack of radios and television will prevent most Afghanis from hearing any U.S. message.
- Civil Affairs: Traditional CA missions would be greatly applicable directly to people of Afghanistan because the country has no infrastructure left after twenty-one years of war. Roads, sewers, water, schools, training the local police, etc. would build good will towards the U.S. and eventually the new government of Afghanistan.

- Counter-Intelligence: CI would have little effect on the Afghani population because they currently support the Northern Alliance and the United States' actions against the Taliban and al Qaeda.
- PSYOP: Traditional PSYOP methods (leaflets, loudspeakers) are some of the best ways to broadcast information in general. An effective campaign could be waged that would entice the Afghanis to support and help the U.S. This would have minimal impact unless cartoon leaflets or small radios were provided because most people can't read and don't have radios.
- Deception: Deception would have little effect on the Afghani population of 26 million. This is based on the assumption of that limited communications would prevent a single story being presented across the country, so a regional or tribal approach would have to be devised. This adds complexity and time to complete a successful deception.
- Computer Network Exploitation: CNE would have little effect on the Afghani people because they have little to no computer infrastructure.
- Computer Network Attack: CNA would have little effect on the Afghani people because they have little to no computer infrastructure.
- Electronic Warfare: If EW was targeted only at the Taliban communication methods but avoided other systems, then the Afghanis could reestablish communication systems (telephone, radio) within their country.

Afghan Population	
Public Affairs (PA)	*
Counterpropaganda (CP)	*
Civil Affairs (CA)	***
Counterintelligence (CI)	*
Psychological Ops (PSYOP)	*
Deception	*
Computer Network Exploitation (CNE)	-
Computer Network Attack (CNA)	-
Electronic Warfare (EW)	**
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 17. Applicability of IO directed toward the Afghan population.

4. Other Islamic States

It is important to look beyond racial considerations and identify how the message presented by the U.S. could affect all nations with large Muslim populations, not only the Arab nations. This focus on populations within other nations highlights the dynamics affecting the U.S-led anti-terrorism coalition formed after the terrorist attacks of September 11, 2001. The coalition is like any other diplomatic arrangement; it depends on the perceived benefits to its participants. This dynamic requires the U.S. to carefully examine every action it takes, including IO. The potential applicability of the IO tools is described below and summarized in Figure 18.

- Public Affairs: A robust PA effort would be the most applicable of the IO tools. A constant flow of accurate and timely information to the world could ensure greater acceptance of unilateral U.S. military actions by the anti-terrorism coalition member states, especially the Islamic ones.
- Counter-Propaganda: This would have limited applicability because a strong PA function would thwart any propaganda campaign by a terrorist organization.
- Civil Affairs: CA actions would have little applicability because they wouldn't affect the way Islamic countries responded to American actions. The U.S. could use CA actions to strengthen its relationship to that country, but this would be no guarantee of support in the war on terrorism.
- Counter-Intelligence: CI would have little applicability against other Islamic countries unless the countries were involved in collecting intelligence on U.S. interests.
- PSYOP: PSYOP could have some effect if creative campaigns were designed to convince both the government leaders of the Islamic countries and the people of the Islamic world of the true goals of the U.S. war against terrorism. This dual focus is required to encourage a common perception of U.S. actions at both the governmental and individual levels.
- Deception: A deception campaign could be a short-term success; but if the deception were compromised, the Islamic world would no longer trust the U.S. at its word. Because of the high risk to the long-term relationships, it is our assessment that the U.S. should not start a deception campaign.
- Computer Network Exploitation: CNE would have little applicability on friendly Islamic countries. Exploitation could be done if known terrorists were using the Islamic country's networks and the country didn't have the capability to exploit the data themselves.
- Computer Network Attack: CNA would have little applicability on friendly Islamic countries. A CNA could be carried out through an Islamic

county's networks if known terrorists were using them and the country didn't have the capability to attack the terrorist's networks themselves or if political sensitivities within that country preclude it from sharing the information. This would likely be a high-risk situation (based on blowback if U.S. action was revealed) and would require a high gain to offset this risk.

- Electronic Warfare: EW would not be applicable against Islamic countries supporting the anti-terrorism coalition actions.

Other Islamic States	
Public Affairs (PA)	***
Counterpropaganda (CP)	*
Civil Affairs (CA)	*
Counterintelligence (CI)	*
Psychological Ops (PSYOP)	**
Deception	-
Computer Network Exploitation (CNE)	*
Computer Network Attack (CNA)	*
Electronic Warfare (EW)	-
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 18. Applicability of IO directed toward other Islamic states.

5. Non-Aligned Countries

There are only a few countries that haven't committed themselves to the principles of the anti-terrorism coalition led by the U.S. Most countries had or have recently committed to the various United Nations treaties on counter-terrorism and have agreed to take the internationally sanctioned anti-terrorism actions, but the U.S. must consider the unintended consequences of its IO campaign to the rest of the world. A summary of the assessments is found in Figure 19.

- Public Affairs: Just like other Islamic states, a robust PA effort would be a highly applicable IO tool. A constant flow of accurate and timely information to the world could ensure greater acceptance of unilateral U.S. and/or allied military actions.
- Counter-Propaganda: Counter-propaganda would allow the U.S. to refute various allegations and limit any perceptions on impropriety made by a non-allied country.

- Civil Affairs: CA would have no applicability because countries have to be on good terms with the U.S. to receive support through a CA program.
- Counter-Intelligence: CI would definitely be applicable. The U.S. would have to step up its CI activities to ensure non-allied countries don't become havens for terrorists or their organizations.
- PSYOP: PSYOP could have some effect if a program was developed to convince the population and governments to join the coalition.
- Deception: A deception campaign would have little effect on a non-allied country because these countries are already resistant to U.S. actions. There could be some deceptions that would motivate a state to join the anti-terrorism coalition, but there is a medium level of risk it could backfire and cost the U.S. some prestige/influence.
- Computer Network Exploitation: Exploitation would be of little overall effect unless the U.S. could find some information that the non-allied countries are supporting the terrorists or their organizations. Once again there is some risk of blowback if the exploitation actions were discovered.
- Computer Network Attack: CNA would not be applicable unless the country becomes a terrorist supporting entity.
- Electronic Warfare: EW would not be applicable unless the country becomes a terrorist supporting entity.

Non-Aligned World	
Public Affairs (PA)	***
Counterpropaganda (CP)	***
Civil Affairs (CA)	-
Counterintelligence (CI)	***
Psychological Ops (PSYOP)	**
Deception	*
Computer Network Exploitation (CNE)	*
Computer Network Attack (CNA)	-
Electronic Warfare (EW)	-
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 19. Applicability of IO direct toward non-allied countries.

6. U.S. Allies in the war on terrorism

With few exceptions, the world has united against terrorism. The level of support to the U.S. led coalition against terrorism is an historic first. The coalition is made up of countries with varied political ideologies and motivations that all need to be addressed. The U.S. has to be especially careful in implementing any IO capabilities and tools that might offend or alienate a coalition partner. There is a difference in the strategic relationship between the U.S. and its traditional allies, like Britain, and the relationships between the U.S. and the other anti-terrorism coalition partners. The long-term allies could be less offended by what would be perceived as offensive or deceptive information operations. Coalition partners most likely would terminate their participation and be more reluctant to join coalitions in the future. The assessments were made based on a middle ground expected reaction. A summary of the assessments is presented in Figure 20.

- Public Affairs: The ability of the U.S. to provide accurate and timely information to all of its allies would greatly enhance the cohesion of the anti-terrorism coalition.
- Counter-Propaganda: A U.S. counterpropaganda effort would guarantee that the allies received accurate information to act upon and not just unconfirmed reports from terrorists or their supporting countries.
- Civil Affairs: Direct CA actions in allied countries would have no effect on the battle against terrorism.
- Counter-Intelligence: The U.S. should limit its CI efforts and use it to monitor the situation in allied countries to prevent any type of espionage or sabotage.
- PSYOP: PSYOP would be somewhat applicable on allied countries. The U.S. could selectively release information to allied countries to ensure their continued support of the coalition. This is a high-risk policy decision that could have considerable blowback and damage strategic relationships quite easily.
- Deception: Outright deception of allies wouldn't be applicable. This may sound hypocritical after the assessment for PSYOP, but there is a subtle difference between the two. It comes down to just prolonging allies' access to all of the information as opposed to outright deceiving them.
- Computer Network Exploitation: CNE is not applicable for use against allied countries.
- Computer Network Attack: CNA is not applicable for use against allied countries.

- Electronic Warfare: EW is not applicable for use against allied countries.

Allies	
Public Affairs (PA)	***
Counterpropaganda (CP)	***
Civil Affairs (CA)	-
Counterintelligence (CI)	*
Psychological Ops (PSYOP)	**
Deception	-
Computer Network Exploitation (CNE)	-
Computer Network Attack (CNA)	-
Electronic Warfare (EW)	-
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 20. Applicability of IO directed toward allies.

7. U.S. Public

An information operations campaign in the United States should be based on giving the American public timely and accurate information. Decision makers must consider the national and military security ramifications of releasing information to the world. There may be instances when it is inappropriate to release certain information about government or military operations to protect the participants. This should be the exception rather than the rule. A continuing debate rages between operational security requirements and the media's belief in the "right " to know. This analysis took the middle ground of the issues involved. A summary of the assessments is presented in Figure 21.

- Public Affairs: PA is the best IO tool to use "against" the American public. Presenting them with accurate and timely information should continue to garner their support for U.S. actions.
- Counter-Propaganda: Counter-propaganda is directly applicable to keeping accurate information in front of the American public to ensure their continued support.
- Civil Affairs: Although National Guard disaster recovery acts could be argued as CA activities to the American population, CA right now supporting U.S. citizens would have no effect on the war on terrorism.
- Counter-Intelligence: CI would have some effect to ensure other nations or groups aren't planning to attack more U.S. targets. This type of activity

would be handled by the FBI and would involve some invasive policing actions that require Federal level approval.

- PSYOP: PSYOP against Americans is prohibited.
- Deception: Deception of the American public is not recommended. Eventually someone will find out and there will be a significant political blowback. Consider the media's reactions after the "left hook" in DESERT STORM when it was revealed that the Marine assault was a deception.
- Computer Network Exploitation: CNE would cause a similar political outrage about individual civil rights and isn't recommended. But the FBI is currently doing some CNE on email servers with a program called Carnivore but only after receiving court orders approving the actions (Johnson, 2001).
- Computer Network Attack: CNA is not advised against the U.S. population in general.
- Electronic Warfare: EW should not be an option against the U.S. population in general. It would take extraordinary circumstances for EW to occur within the U.S.

U.S. Public	
Public Affairs (PA)	***
Counterpropaganda (CP)	***
Civil Affairs (CA)	-
Counterintelligence (CI)	**
Psychological Ops (PSYOP)	-
Deception	-
Computer Network Exploitation (CNE)	-
Computer Network Attack (CNA)	-
Electronic Warfare (EW)	-
- No Effect * Little Effect ** Some Effect *** Great Effect	

Figure 21. Applicability of IO directed toward U.S. population.

8. IO Mix Conclusion

When the individual category assessments are compiled into a single color matrix, an interesting pattern appears (see Figure 22). First, it becomes apparent that the current U.S. emphasis on CNE, CNA, and EW, is shortsighted and doesn't consider the effects

the other six OIO tools could have on an opponent. The U.S. isn't benefiting from the synergy a coherent information strategy could provide. Secondly, and quite surprisingly, the composite matrix vividly shows that the current U.S. strategy based on CNO and EW ignores or minimizes over two thirds of the world audience.

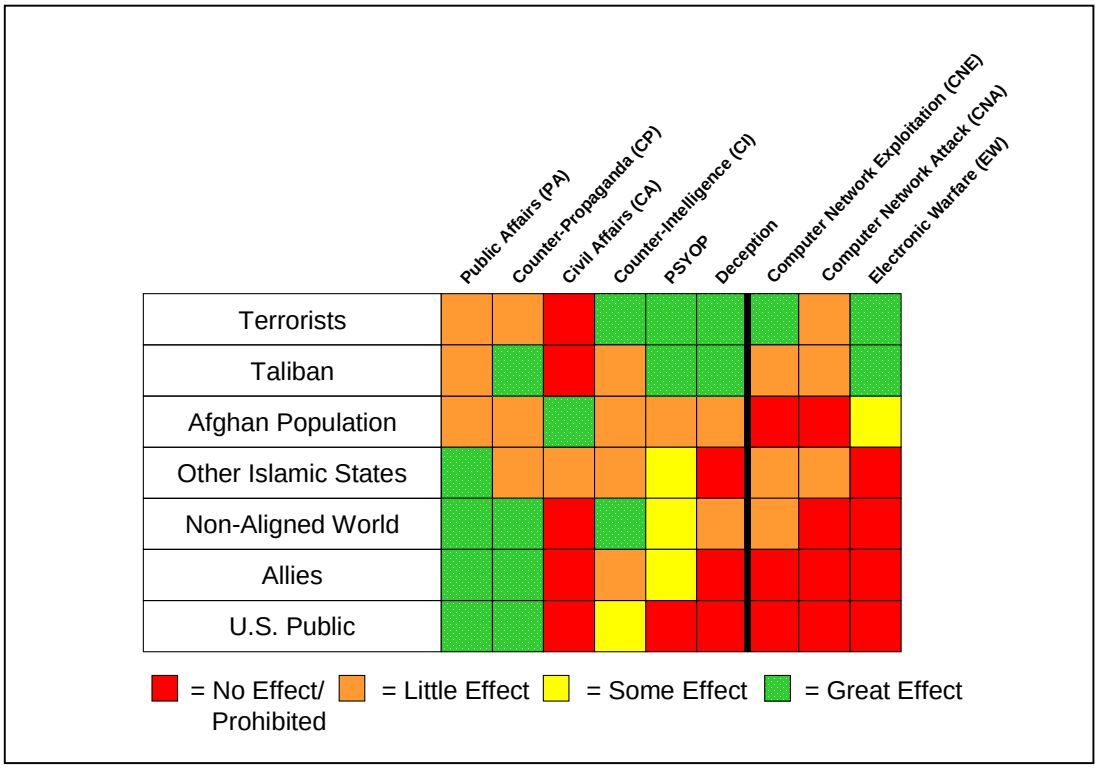

Figure 22. Composite analysis matrix.

B. EXECUTION AND EVALUATION

The last two steps of the IO planning methodology are the execution of the plan and monitoring its progress and the evaluation of the execution to make the required changes in the next iteration of the IO plan. The Administration did these two steps fairly well. They were careful to monitor how information played on the world stage and modified their approach based on the feedback from the original message. The consistent reassurance of the worldwide Muslim community was a perfect example. The Administration adjusted the message and method many times based on feedback from other world governments and the Muslim community.

C. CONCLUSION

The ten step sequence in our IO planning methodology seems to capture the essential decisions to be made when crafting a policy and a plan for the informational aspect of national power. The Bush Administration's actions in response to the terrorist attacks on September 11, 2001 resemble the logic of the IO planning methodology presented in this chapter. But the emphasis on CNA, CNE, EW, and poorly executed perception management was self-limiting. The analysis suggests that the U.S. could have initially been much more effective in the infosphere if it had focused its message and used all the IO capabilities at its disposal.

It is worth mentioning that the Administration realized the shortfall in its ability to project our message to the rest of the word and decided to create the Office of Strategic Information within the Department of Defense. The office was to "set up policies for information operations and warfare that will then be carried out by military specialists to 'influence the hearts and minds of the opposition'" ("New Pentagon Office", 2002). The biggest problem initially identified would "be coordinating with the Pentagon's public affairs operation, the State Department's overseas diplomacy program and the White House's 'war room' ("New Pentagon Office", 2002). But the office died a political death within four days of its announcement when the press widely reported that the main purpose of the office was to intentionally mislead foreign media. Secretary Rumsfeld realized that the office would not survive all the bad press and be effective, so decided to close it. He did say that information operations and strategic influence operations would continue, "just in different offices" ("Pentagon closes", 2002).

The next chapter will suggest a possible solution to ensure all of the information capabilities are considered in the future both at the national and Department of Defense level.

THIS PAGE INTENTIONALLY LEFT BLANK.

V. SUMMARY AND CONCLUSION

A. SYNOPSIS

In this thesis we have explored the idea that a national information strategy would enhance the effectiveness and breadth of military operations, specifically military information operations. We started with a discussion of the importance of information and how easily it is moved, manipulated, and compiled by anyone with access to a personal computer and a phone line. After reviewing current thinking on the future of information in war, we determined that any information strategy or policy must address, at a minimum, the areas of perception management, system destruction, and information exploitation.

To provide a theoretical foundation, we defined information and information operations by first examining how information becomes understanding. The IO Information Pyramid illustrated this process. We then defined information operations and discussed how IO could be used in conjunction with military operations to meet national security goals. Specifically, this thesis proposed a National Information Strategy, similar in use as the National Security Strategy, to provide direction to all the departments and agencies in the U.S. government on the informational aspect of national power.

A National Information Strategy would coordinate the message the government is trying to send to all the audiences interested in a particular issue. We discussed how the information strategy would have to be flexible, scalable, and adaptable to address the myriad of different situations. The strategy would provide direction about: 1) the message to be passed, 2) the intended audience(s), 3) the unintended audience(s), 4) how to pass the message, and 5) how to prevent an opponent from doing the same with their message.

Next we looked at how to use the 17 IO capabilities. First we divided the capabilities into the four categories: information assurance, wetware standardization, deny/disrupt/destroy operations, and perception management. Then we examined each category discussing each capability and how it could be used to meet the IO objectives and goals of the campaign at the strategic, operational, and tactical levels of war.

Armed with a concept of how to use each IO capability, we needed to identify the way to plan to use IO. Current joint publications provide only operational and tactical-level planning guidance for military organizations. There is no method or tool to assist in the comprehensive planning of IO at the strategic level. So we looked to business for a method or model that might apply. We took a marketing planning methodology and with a little modification, we were able to include all the planning elements necessary for IO.

To validate our new methodology, we compared it to how the Administration reacted in the infosphere to the terrorist attacks on September 11, 2001. From the speeches, press conferences, interviews, and policy statements, the Administration seemed to use a similar methodology as in our planning methodology. The only shortfall we identified in the Administration's response was the mix of IO capabilities. So we designed a method to determine which IO capabilities were the most applicable to the target and incidental audiences.

After completing the IO capabilities mix analysis, we determined that the national security community, including the Department of Defense, limited themselves to CNE, CNA, some PSYOP and EW based on publicly reported accounts of the resulting military operations. We concluded that this narrow focus prevented the U.S. from receiving the full benefit of the other capabilities and it limited the "range" of IO to only one third of the potential target audiences of the world.

B. CONCLUSIONS

The lack of understanding of what information is and the diffuse characteristics of the infosphere may have prevented the U.S. from leveraging all of its capabilities in times of conflict. The U.S. response to the terrorist attacks on "9/11" focused on the technology and deny/disrupt/destroy, and some of the perception management paradigms. But the attempts at perception management were not done skillfully (e.g., calling the U.S. response a "crusade"). These types of missteps required time to overcome. Additionally, the United States and its allies missed many opportunities to affect the "battle of the story" by not properly identifying all the target audiences and not considering the effects of its message on the unintended audiences.

Many of the problems identified are a result of the lack of national-level direction for the informational capabilities of the country. Current informational goals are encapsulated within the National Security Strategy, but they only focus on the information infrastructure of the country and are mute about perception management. This thesis proposes two tools to address these problems: a National Information Strategy and an IO strategy methodology.

1. A National Information Strategy

To demonstrate the importance of information, a separate National Information Strategy (NIS) could be written to provide specific informational objectives and goals for all the departments and agencies of the U.S. government. The current method of putting some informational objectives and goal in the National Security Strategy (NSS) does not adequately highlight the importance of information in today's environment. A NIS would provide direction at the macro level for information and it would emphasize the use of all 17 of the IO capabilities available to the United States. The NIS, like the NSS, would be written as a summary of the national interests and values to clarify national policies and policy statements specifically about information (see Figure 23).

The NIS would then be used by each department and agency to craft their own information strategies. By using this method, every organization would be in synchronization with the Administration. The NIS process would allow the Administration to learn how each department or agency plans to implement the national information policies.

The DOD would create a National Military Information Strategy (NMIS) outlining how the military IO capabilities would be used to meet the national information goals. As a separate document from the National Military Strategy, the NMIS would highlight the importance of information and the need for the services to address all of the IO capabilities in their doctrine, plans, programs and budgeting. Theater commanders would then use the NMIS to develop their theater IO strategies and plans, guaranteeing alignment with the Administration's informational objectives and goals.

The National Information Strategy would address a three- to five-year period like the National Security Strategy, but there would be a process to issue Addenda to the

strategy in response to crises or emerging technologies that alter the NIS. The Addenda would be used by the Administration to provide timely informational direction to the departments and agencies. It would not be used as a public affairs type notice; the Addenda would provide informational policy guidance to the government's departments and agencies concerning the particular issue or event.

A National Information Strategy concept would prevent the conflicting "official positions" that are often encountered in the midst of a crisis. This happens because one agency states a position and then another states a different position causing great confusion as to where the United States really stands on an issue. This type of confusion can merely be embarrassing to the Administration or it could cause an adversary to misunderstand our intent in a crisis.

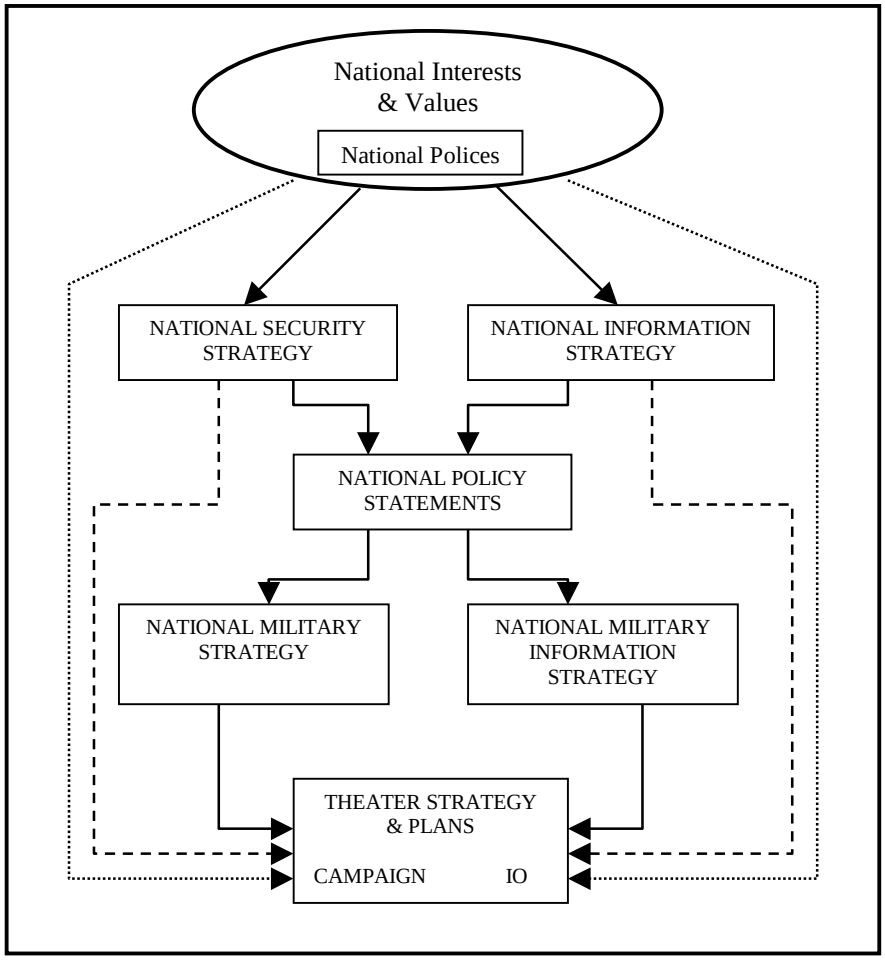

Figure 23. National Strategic Direction with Information.

2. Information Strategy Methodology

The IO planning methodology presented in Chapter III is a simple but effective tool that anyone who is developing IO strategy can use. It provides a checklist approach to the key areas and concepts to be considered in the formulation of an information strategy. This ensures no area is missed and the resulting strategy is broad enough to allow creative execution and innovation, but bounded enough to focus any effort taken in support of the strategy. The following excerpt from the Public Diplomacy section of *A National Security Strategy for the Next Century* is an example of how the boundaries of a strategy are presented,

> Effective use of our nation's information capabilities to counter misinformation and incitement, mitigate inter-ethnic conflict, promote independent media organizations and the free flow of information, and support democratic participation helps advance U.S. interests abroad. ("A National Security Strategy", 1999, p. 6)

In this case, it should be relatively easy for the State Department to take this macro level direction and craft its own information strategy so its public diplomacy efforts meet the objectives and goals presented in the National Security Strategy or in a National Information Strategy as previously suggested.

These two tools, a National Information Strategy and the IO planning method may allow the U.S. to effectively use all of it superior information capabilities in support U.S. interests and allow the country to keep the lead in the global "battle of the story."

C. AREAS FOR FURTHER RESEARCH

As this thesis progressed numerous ideas for further research emerged. Below is a list of only a few of them that could have the most impact on the evolution of information operations doctrine, and practice.

- Use the composite matrix concept as the situation analysis tool to assess the strategic information environment.
- Are there any lessons to be learned from past implementations of centralized information or theme processes? Does centralization eliminate creativity and innovation?

- How would a National Information Strategy affect the relationships among public affairs, intelligence, and operations in the military?
- At what point could the National Military Information Strategy and the National Military Strategy be integrated into a single document? Which would take precedence?
- How should military officers be educated about strategic information operations and its planning process? Would training be sufficient?
- Create the sub-area questions for the IO planning method steps and compile them into what could become a joint publication.

APPENDIX A. GLOSSARY

Civil affairs. The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Also called CA. (JP 1-02)

Computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (This term and its definition are approved for inclusion in the next edition of JP 1-02.)

Computer network exploitation. Intelligence collection and enabling operations to gather data from target adversary automated information systems (AIS) or networks. Also called CNE. (This term and its definition has been taken from the Draft DoD Directive 3600.1, Oct 2001).

Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 1-02)

Data management: The control of data handling operations--such as acquisition, analysis, translation, coding, storage, retrieval, and distribution of data--but not necessarily the generation and use of data. (Institute for Telecommunication Sciences, Boulder, CO. Available at http://www.its.bldrdoc.gov/fs-1037/dir-010/_1432.htm)

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (JP 1-02)

Electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams, or anti-radiation weapons). b. electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronic intelligence. (JP 1-02)

Information assurance: Information operations (IO) that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction

capabilities. (Institute for Telecommunication Sciences, Boulder, CO. Available at http://www.its.bldrdoc.gov/projects/devglossary/_information_assurance.html)

Information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)

Infosphere. The infosphere refers to the rapidly growing global network of military and commercial command, control, communications, and computer (C4) systems and networks linking information data bases and fusion centers that are accessible to the warrior anywhere, anytime, in the performance of any mission. (JP 6-0)

Perception management — Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. See also psychological operations. (JP 1-02)

Psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

Public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (JP 1-02)

Special information operations. Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also

called SIO. (This term and its definition are approved for inclusion in the next edition of JP 1-02.)

LIST OF REFERENCES

Adams, J. (1998). *The Next World War*. New York, NY: Simon & Schuster.

Afghanistan. (2001, 16 Dec). New York: Learning Network. Available at http://www.infoplease.com/ipa/A0107264.html.

Afghanistan: Country Profile (2001, 10 December). London, U.K.: British Broadcasting Company. Available at http://news.bbc.co.uk/hi/english/world/south_asia/country_profiles/newsid_1162000/1162668.stm

Alexander, J. B. (1999). *Future War: Non-Lethal Weapons in Twenty-First Century Warfare*. New York, NY: St. Martin Press.

A National Security Strategy For A New Century (1997, May). Washington, DC: The White House, Office of the President of the United States.

"And Bomb the Anchovies" (1990, August 13). p. 13. New York, NY: *Time*, Available at http://www.time.com/time/searchresults?summaries=yes&search_type=simple&query=bomb+the+anchovies&venue=timemags%7Cmagazine

Arquilla, J. (2001, March). *Conflict in an Information Age* (Unpublished notes from a graduate seminar lecture). Monterey, CA: Naval Postgraduate School.

Arquilla, J. & Ronfeldt, D. (Eds.). (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: The Rand Corporation.

Bush, George W. (Speaker). (2001, September 11). (Radio address from Barksdale AFB, LA). Available at http://www.globalsecurity.org/military/library/news/2001/09/mil-010911-2f611b09.htm

"Bush gets strong support from Congress, NATO" (2001, September 12). Atlanta, GA: Cable News Network. Available at http://www.cnn.com/2001/US/09/12/america.under.attack/index.html

Carpenter, T. G. (2001, September 26). *A War, Not a Crusade*. Washington, DC: Cato Institute. Available at http://www.cato.org/current/terrorism/pubs/carpenter-010926.html

CISCO Systems (2001, April 26). *Increasing security on IP Networks*. San Jose, CA: Author. Available at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

CISCO Systems (2002, February 20). *Network Management Basics*. San Jose, CA: Author. Available at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm#xtocid3

Clausewitz, C. (1983). *On War*, A. Rapoport, Ed., J. J. Graham, Trans. Harmondsworth, U.K.: Penguin. (Original work published 1832; Graham translation in 1873; includes elements of 1908 F.N. Maude edition).

Ford, P. (2001, Sep 19). "Europe cringes at Bush 'crusade' against terrorists". Boston, MA: *The Christian Science Monitor*. Available: http://www.csmonitor.com/2001/0919/p12s2-woeu.html

Haddah, W. Z. (1993, October). *The Crusaders thru Muslim Eyes*. Available at http://www.geocities.com/Athens/Troy/9663/crusaders.html

Heibing, R. G. & Cooper, S. W. (1996). *The successful marketing plan* (2nd Ed.). Lincolnwood, IL; NTC Business Books.

Joint Staff (2001, Deccember 19). *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*. Washington, DC: Author.

Joint Staff (2001, September 10). *Joint Publication 3-0, Doctrine for Joint Operations*. Washington, DC: Author.

Joint Staff (1998, October 9). *Joint Publication 3-13, Joint Doctrine for Information Operations*. Washington, DC: Author.

Joint Staff (2000, April 7). *Joint Publication 3-51, Joint Doctrine for Electronic Warfare*. Washington, DC: Author.

Joint Staff (1996, May 31). *Joint Publication 3-58, Joint Doctrine for Military Deception*. Washington, DC: Author.

Joint Staff (1997, May 14). *Joint Publication 3-61, Doctrine for Public Affairs in Joint Operations*. Washington, DC: Author.

Katzman, K. (2001, Sep 10). *Terrorism: Near Eastern Groups and State Sponsors, 2001*. Washington, DC; Congressional Research Service. Available at http://www.fas.org/irp/crs/RL31119.pdf

Libicki, M. & Shaprio, J. (1999). *Conclusion: The Changing Role of Information Warfare*. In Z. Khalilzad (Ed.), *Strategic Appraisal: The Changing Role of Information in Warfare* (pp. 437-452). Santa Monica, CA: The Rand Corporation.

McCaleb, I. C. (2001, October 12). "U.S. airstrikes slam multiple Afghan targets". Washington, DC: Cable News Network. Available at http://www.cnn.com/2001/US/10/11/ret.attack.pentagon/

McIntyre, J. (1996, March 2). *China fires another missile: Tense U.S. monitors war games off Taiwan*. Atlanta, GA: Cable News Network. Available at http://www.cnn.com/WORLD/9603/china_taiwan/12/pm/

Miller, A., Jefferson, M., & Rodgers, J. (2001, July). "Global Information Grid." *The Edge, Vol. 5, No. 2*, ¶ 6. Available at http://www.mitre.org/pubs/edge/july_01/miller.htm

"New Pentagon office to spearhead information war" (2002, February 20). Washington, DC: Cable News Network. Available at http://www.cnn.com/2002/US/02/19/gen.strategic.influence/

"Terror Plot in Works 5 years" (2001, September 14). West Palm Beach, FL: NewsMax. Available at http://www.newsmax.com/archives/articles/2001/9/ 14/101424.shtml

"Pentagon closes down controversial office" (2002, February 26). Washington, DC: Cable News Network. Available at http://www.cnn.com/2002/US/02/26/defense.office/

Salkever, A. (2002, March 12). "Hacking al Qaeda's Secrets". Washington, DC: *BusinessWeek*. Available at http://www.businessweek.com/bwdaily/dnflash/mar2002/ nf20020312_9960.htm

"September 11 warnings: Who knew what, and when?" (2002, May 24). Atlanta, GA: Cable News Network. Available at http://www.cnn.com/2002/US/05/22/9.11.warnings.facts/index.html

Shalikashvili, J. M. (1997, May). *Shape, Respond, Prepare Now -- A Military Strategy For A New Era*. Washington, DC: Joint Chiefs Of Staff.

Sieberg, D. (2001, Sep 21). *Bin Laden exploits technology to suit his needs*. Atlanta, GA: Cable News Network. Available at http://www.cnn.com/2001/US/09/20/ inv.terrorist.search/

Slabodkin, G. (1998, November 9). *Navy: Calibration flaw crashed Yorktown LAN*. Washington, DC: Government Computer News. Available at http://www.gcn.com/ archives/gcn/1998/november9/6.htm

Starr, A. (2001, December 17). "Charoltte Beers' toughest sell." Washington, DC; *BusinessWeek*, pp. 56-58.

Taliban. (2001). New Delhi, India: South Asia Terrorism Portal. Available at http://www.satp.org/satporgtp/usa/Taliban.htm#

Tenet, G. J. (2000, February 2). *The Worldwide Threat in 2000: Global Realities of Our National Security Strategy* (Testimony before the Senate Select Committee on Intelligence). Washington, DC: Author. Available at http://www.mipt.org/dci020200.html

United States Air Force (1998, August 5). *Air Force Doctrine Document 2-5, Information Operations.* Washington, DC: Author.

United States Army (1996). *Field Manual 100-6, Information Operations*. Washington, DC: Author.

United States Government Services Administration, Information Technology Service (1996, August 7). *Glossary of Telecommunications Terms (Federal Standard 1037b)*. Washington, DC: Author. Available at http://www.its.bldrdoc.gov/fs-1037/

Williams, R. (2001, November 28). "Their Troops Quit When Taliban, Al Qaeda Leaders Break." Washington, DC: American Forces Press Service http://www.defenselink.mil/news/Nov2001/n11282001_200111282.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. John Arquilla
   Naval Postgraduate School
   Monterey, California

4. Prof. Dan Boger
   Naval Postgraduate School
   Monterey, California

5. Jennifer Duncan
   Naval Postgraduate School
   Monterey, California

6. Deputy Director of Information Operations
   Joint Staff
   Pentagon, Virginia

7. Commander
   United States Special Operations Command
   MacDill AFB, Florida

8. Commander
   Air Force Special Operations Command
   Hurlburt Field, Florida