NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

INFORMATION OPERATIONS IN STRATEGIC, OPERATIONAL, AND TACTICAL LEVELS OF WAR: A BALANCED SYSTEMATIC APPROACH

by

Bunyamin Tuner

September 2003

Thesis Advisor:	Daniel Boger
Thesis Co-Advisor:	Steve Iatrou

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** September 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Information Operations In Strategic, Operational, And Tactical Levels Of War: A Balanced Systematic Approach			**5. FUNDING NUMBERS**
6. AUTHOR(S) Bunyamin Tuner			
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**

13. ABSTRACT ***(maximum 200 words)***

This thesis explores the idea whether a balanced systematic approach is a better way to integrate Information Operations (IO) at different levels of war compared to uncoordinated efforts at each level. Analysis of the role of information in a conflict in the context of information superiority provides the foundation of the thesis. DOD's IO core, supporting, and related capability based approach was used in the analysis of each level of warfare. Strategic, operational, and tactical level IO were analyzed by matching relevant IO capabilities with the IO effects desired at the respective levels. Sample systems were provided for each capability when appropriate. IO efforts in Operation Desert Storm and Operation Allied Force were analyzed. This thesis concluded that a balanced systematic approach to IO through its integration at all three levels of warfare will produce much better results than the uncoordinated cases in order to exploit the integrative effect of IO on the instruments of national power and the military capabilities at different levels of warfare.

14. SUBJECT TERMS Information Operations, information superiority, levels of warfare, Operation Desert Storm, Operation Allied Force			**15. NUMBER OF PAGES** 89
			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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

INFORMATION OPERATIONS IN STRATEGIC, OPERATIONAL, AND TACTICAL LEVELS OF WAR: A BALANCED SYSTEMATIC APPROACH

Bunyamin Tuner
First Lieutenant, Turkish Army
B.S., United States Military Academy, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2003

Author: Bunyamin Tuner

Approved by: Daniel Boger
Thesis Advisor

Steve Iatrou
Thesis Co-Advisor

Daniel Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the idea whether a balanced systematic approach is a better way to integrate Information Operations (IO) at different levels of war compared to uncoordinated efforts at each level. Analysis of the role of information in a conflict in the context of information superiority provides the foundation of the thesis. DOD's IO core, supporting, and related capability based approach was used in the analysis of each level of warfare. Strategic, operational, and tactical level IO were analyzed by matching relevant IO capabilities with the IO effects desired at the respective levels. Sample systems were provided for each capability when appropriate. IO efforts in Operation Desert Storm and Operation Allied Force were analyzed. This thesis concluded that a balanced systematic approach to IO through its integration at all three levels of warfare will produce much better results than the uncoordinated cases in order to exploit the integrative effect of IO on the instruments of national power and the military capabilities at different levels of warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. INFORMATION OPERATIONS: THE HYPE

It is no wonder that the industrial age witnessed the appearance and dominance of the warfighting machines such as tanks, planes, aircraft carriers, etc. The armed forces of that age became successful by making these machines faster, more lethal and more survivable, and massing them in a coordinated fashion. The industrial age resulted in the ubiquitous existence of these machines in many nations, and caused armed forces to search for better ways to employ what they have using the improvements in technology. We are now the dwellers of the so-called information age. It is no surprise that the terms like Information Operations (IO), Information Warfare, and Information Superiority have become popular as force multipliers. Information is nothing new, but how did we come to the point that it has been perceived as a weapon of some sort in this age? Is it really a silver bullet, or is it just another misconception like the idea before the First World War that "War was obsolete given mankind's level of sophistication?" This thesis does not claim to answer all these questions, but merely tries to shed light on the concept and practice of IO.

The recent success of the US and coalition forces can exemplify the growing excitement about IO. The coalition ground forces in Iraq faced a 3 to 1 or 4 to 1 disadvantage. Although it is a commonly taught principle that an attacker should have a force advantage of at least 3 to 1, the above fact did not hinder the coalition forces much. The bare numbers stripped of other factors make the German Blitzkrieg look primitive: "The Germans managed to conquer France, the Netherlands, and Belgium in just 44 days, at a cost of 'only' 27,000 dead soldiers. The United States and Britain took just 26 days to conquer Iraq (a country 80 percent the size of France), at a cost of 161 dead, making fabled generals such as Erwin Rommel and Heinz Guderian seem positively incompetent by comparison" (Boot 44). Besides mentioning the incompetence of the Iraqi forces as the major factor, Max Boot attributes this success also to proficiency of the US forces in IO. He argues that the US forces "severely disrupted Iraqi command-and-control systems and moved much faster than Iraqi forces could handle" (Boot 51). He also mentions

Network Centric Warfare Capability of the US forces, the effectiveness of C4ISR technologies, and even television propaganda / disruption efforts by both sides, which are all part of IO. Another figure showing the prominence of the IO was that in Operation Iraqi Freedom, the US forces used 30 times more bandwidth than that they used in Desert Storm (Boot 58). Boot concludes that the US military machine will transform into a more efficient one by adapting the information technologies available. As a result, the success in the recent Operation Iraqi Freedom promises that the hype over the IO will continue to increase especially in the US.

A different approach to military technological advancements in the age of "military transformation" deserves mentioning. Stephen Biddle examines 20th Century land warfare and establishes several continuities regarding the effect of technological developments on the art of war. His conclusion is that the technological advancements which occasionally led one side to win an overwhelming victory over its adversary did not cause radical revolutions in warfare. Rapid technological change has been a part of warfare, which was especially true in the 20th century. Instead of clear discontinuities, efficiency in battlefield spiraled around several continuities: "Again and again, armies have returned to a body of tactical and doctrinal principles that arose almost with the dawn of the era of modern firepower at the turn of the twentieth century. In an extended process of trial by fire, the concepts of combined arms, tight integration of movement and suppressive fire, aggressive use of cover and concealment, and defensive depth and reserves have repeatedly proven necessary for effective operations on a radically lethal battlefield" (Biddle 107). Each new wave of technology tempted the military minds in assuming that unheard-of new methods would be necessary to cope with them, but they were driven back to the fundamental battlefield tactics by painful experience. Biddle's conclusion, though referring only to land warfare, is applicable to the joint and combined nature of current warfighting:

> Experience suggests a different military change. Rather than new technology creating periodic revolutionary breaks with the past, what technology actually did in the twentieth century was to punish mistakes with increasing severity. The more deadly the weapons and the more effective the information-gathering systems for locating their targets, the more painful has been the failure to adopt traditional cover, concealment, combined arms, and suppressive fire tactics. The faster and longer range

> the combat vehicles, the more damaging has been the failure to adopt depth and withhold sufficient forces in reserve. Armies that have failed to master these methods have suffered increasingly one-sided defeats since 1900. Armies that have implemented such methods, however, have been able to insulate themselves from the worst effects of new weapon technologies…. Technological change in land warfare can thus be thought as a wedge, driving apart the real military capability of armies that can, from those that cannot, implement the complex canon of orthodox modern tactics and doctrine (Biddle 110).

The author of this thesis believes that IO is another evolutionary step in warfighting, which allows the forces to better integrate and to more efficiently utilize the principles of warfare. It will give an edge to the forces that master it against those who fail to implement it.

B. OVERVIEW – SCOPE OF THIS STUDY

The purpose of this thesis is to examine information operations and systems used in IO at different levels of war, and to emphasize the need to balance their use in search for efficiency and success promised by IO. The primary research question examined in this thesis is whether a balanced integration of Information Operations (IO) in different levels of war -- strategic, operational, and tactical – is better than uncoordinated efforts in each level. The answers to the following research questions will pave the way to answer the primary research question:

- What is IO and how does it differ in different levels of war?
- How does IO in each of these levels contribute to the overall success of the IO campaign?
- What are sample systems contributing to the IO effort in different levels of war?
- How can we integrate IO efforts in different levels of war?
- What are the possible consequences of integrated/uncoordinated IO for the overall IO campaign? Which is better?

C. KEY DEFINITIONS AND CONCEPTS

1. Key Definitions

A few terms deserve defining in the realm of IO:

Information Operations (IO): Actions taken to affect adversary information and information systems while defending one's own information and information systems.
Information Warfare (IW): Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.
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.
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 (Joint Publication 3-13 GL-7).
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 1-02 261)

2. What is Information Operations?

As the above definitions suggest, IW is only the portion of IO which takes part during time of crisis or conflict. The literature on IO recommends implementation of IO before a crisis situation occurs and for a while after the level of intensity decreases, which is believed to improve efficiency during crisis and to bring about a sooner and more permanent resolution. This article will focus on IO as it pertains to both peacetime and conflict situations. The above definition of IO is what Joint Doctrine for Information Operations, published in 1998, presents. However, this definition also seems to be a working one because IO is still brand new and under construction -- in Internet terms. The 1990's have seen several versions of IO definitions by different services and the 21st century has not yet perfected our understanding of IO (Alger 4).

While IO is a brand new term, it has been a part of warfare and politics in the past, but was not branded as such. The Information Warfare Site[1] provides a timeline for IO and starts the timeline at 1200 BC with the Trojan Horse. Operations Husky and Overlord regarding the Normandy Invasion in World War II are some other examples ("JFSC JCIWS IW Division-IO Timeline"). These examples depict cases in which

[1] The Information Warfare Site is a UK based online resource that aims to stimulate debate about a range of subjects from information security to information operations and e-commerce. It can be accessed at http://www.iwar.org.uk/index.htm

manipulating an adversary's information led to successful campaigns. We can try to use these examples to downgrade IO's current importance claiming that IO has been a part of warfare for a long time, but the question remains: What makes it relevant to the military transformation we are going through right now? The following argument tries to explain why:

The military organizations of the past had simpler weapons, technology, organizations, and adversaries to deal with. Nevertheless, our age is witnessing the integration of increasingly complex information systems into traditional warfighting disciplines such as mobility, logistics, command, control, communications, computers, and intelligence. Many of these systems have inherent vulnerabilities which are usually unavoidable consequences of enhanced functionality, interoperability, efficiency, and convenience to users. The advancements in technology make them efficient and cost effective to extend the capabilities (besides vulnerabilities) to an unprecedented number of users. These information systems enhance warfighting immensely. However, these useful capabilities cause dependence, and that dependence creates vulnerabilities. "These information systems are a double-edged sword — on one edge representing areas that warfighting components must protect, while on the other edge creating new opportunities that can be exploited against adversaries or used to promote common interests" (Joint Publication 3-13 I-11). Another aspect of IO that deserves mentioning is its effect on the decision-making cycle. In the ever-increasing speed of warfare, the faster you can decide, the better off you will come out of a conflict. Even this concept is not new. John Boyd was the mind behind the Observe-Orient-Decide-Act (OODA) Loop, and he advocated that you needed to get inside the adversary's OODA Loop in order to win. Either by going through the OODA Loop cycle faster than the opponent or by varying your tempos and rhythms so your opponent cannot keep up with you, you can gain leverage over your opponent and prevent him from gaining leverage over you (Hammond). The current technologies immensely improved situational awareness and the capability to disseminate it to the lowest levels of warfighting, which in return brought Boyd's ideas closer to reality. The fundamentals of affecting an adversary's information and information-based systems and defending one's own have not changed through time. What has changed is the means and route of attack (Air Force Doctrine Document 2-5 ii). As a result, IO has

gained importance as a relevant concept in current military transformation due to inherent vulnerabilities and emerging opportunities.

3. Information Superiority

IO exploits the inherent vulnerabilities and emerging opportunities in order to gain advantage over the adversary, called *Information Superiority.* Information superiority is a prerequisite to making better and faster decisions than the opponent. Superior decision-making resulting in directed and effective actions is the key to affect the will of the opponent, either through its decision makers, its troops, or its public. Affecting the opponent's will is the best way to end the hostilities in a shorter time period and with fewer casualties for the friendly forces. Having in mind the joint doctrine definition of information superiority afore mentioned, Hall provides a more meaningful and functional definition of *Information Superiority*:

> The use of information technology and intellectual power to create conditions to make better and faster decisions than an adversary. These better, faster decisions provide advantages in tempo, initiative, and momentum against an enemy or opponent at a time and place of the commander's choosing, with the notion of creating conditions leading to the effects most conducive to rapid mission accomplishment and sustainment of advantage, at minimal cost (Hall 59).

In order to make the advantages attained through information superiority more tangible, we will use Edward Waltz's model for information warfare by extending it to contain peacetime activities of IO (4). Then we will introduce several types of advantages gained through information superiority.

4. A Basic Engagement Model

In this basic scenario, countries A and B are engaging each other. In a conventional understanding, A is the attacker, and B is the defender. The objective of A is to influence and coerce B to act in a way favorable to A's interests (i.e., to cause B to surrender, to cease from hostilities, to withdraw forces, etc.). Three major factors influence B's decisions and resulting actions / reactions to A's actions:

- *The capacity of B to act*: This is a physical factor and often a limiting constraint on a country to perform certain actions. It can be measured in terms

of capability to command and strength of force. For example, a country needs to have certain platforms before it can conduct strategic mobility. Attrition warfare is based on the idea that degradation of B's warfighting capability will eventually cause B to make decisions in line with attacker's objectives.

- *The will of B to act*: This element is a human factor and a measure of the resolve or determination of the human decision-makers of B and their inclination towards alternative actions. The will is the hardest for the attacker to measure, model, or directly influence. However, since Sun Tzu's time, it has been regarded as the "supreme excellence" to affect the adversary's will trying to persuade it to comply without fighting.
- *The perception of B*: This element represents the understanding of the situation from B's perspective. It is an abstract information factor and is measured in terms such as accuracy, timeliness, completeness, confidence or uncertainty. B's decisions depend on B's perception of the situation and of its own capacity to act.

A has several alternatives to influence B's actions based on the above factors. A can attack directly to B's capacity to act, which reduces the options available to B and indirectly influences the will of B. A can also influence B's perception of the situation, the constraints to actions, or the possible outcomes of actions (by attacking the capacity of B or its sensors, communications, etc.). A cannot attack the will of B directly, but capacity and perception attacks both provide access points to the will even if limited (Waltz 4).

Waltz's "basic model of the information processes in a conflict between attacker A and defender B" can be seen in Figure 1 (Waltz 6). This model depicts the flow of information from A across four domains to the decisions and actions of B. This model will be the basis of this thesis in approaching where available systems fit in the realm of IO. It will demonstrate the alternatives through which A may influence B's perception.

The first domain is the physical one where B's capacity to act resides. People, resources, weapons platforms, lines of communication, command and control capabilities, etc. belong to the physical domain. Information domain is the electronic

realm where B observes the world, monitors A's activities, communicates with and measures the status of its own forces. In the perceptual domain, B combines and analyzes its observations to perceive the situation or to orient itself. This process also assesses the will, the goals, and the capacity of A while comparing the feasible outcomes of the reactions B may choose with its current observed strength. The human mind is the central element in this domain. The final domain of the human choice and will is where B decides how to act or react. These decisions depend on the perceived situation, alternative actions available, and possible outcomes of those alternative actions. The "heart" of the decision-maker (resolve, determination, human will) is the central element of this domain (Waltz 5).

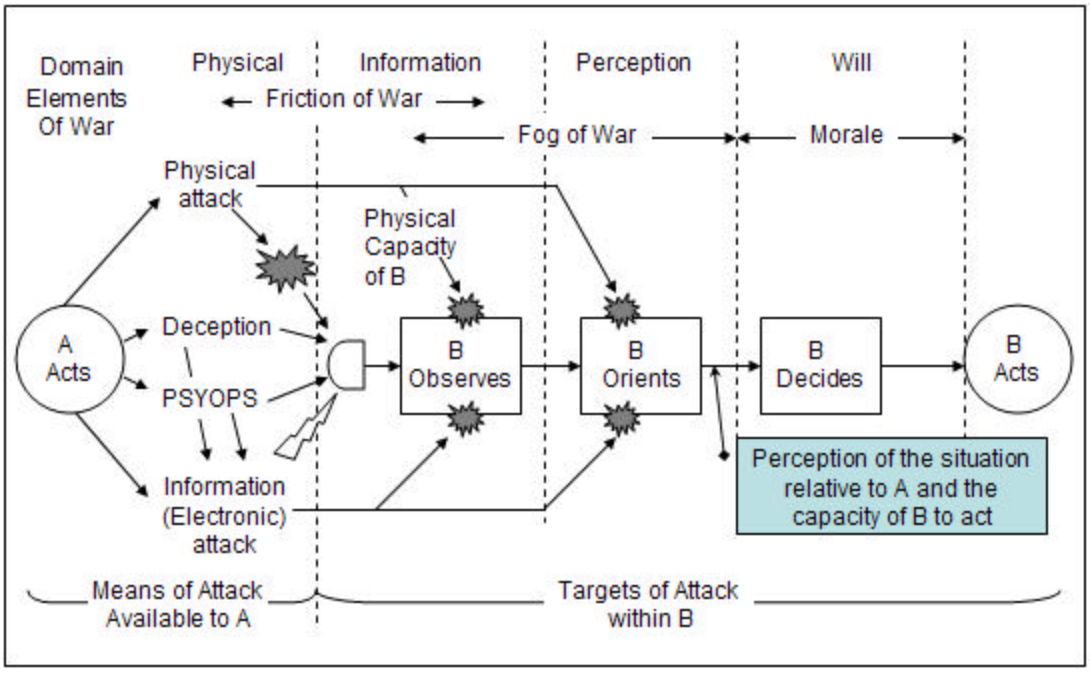

Figure 1. A Basic Model of Information Processes in a Conflict (From Waltz 6)

According to the model shown in Figure 1, A has 4 basic options to influence B's decisions:

Physical Attack: The physical attack may be used in the classical attrition war sense to reduce B's capacity to act (i.e. destruction of bridges, attacking military forces, etc.). It can also be directed towards B's capacity to observe, to orient, to command, or to react with force. Physical attacks on sensors and communications affect B's observation

process while attacks on command nodes affect orientation process. Both types of attacks deny valuable information or corrupt the decision-makers' perspective.

Deception: The goal of deception is to enhance friendly effectiveness by reducing B's effectiveness in both defense and offense. Achieving surprise in attacks and seducing the opponent to take ineffective and vulnerable actions are essential elements of deception.

Psychological Operations (PSYOP): These comprise psychological attacks at human perception seeking to manage or to influence B's perception about the circumstances of the conflict. Psychological Operations are aimed at B's overall ability to perceive while deception desires to induce specific behaviors.

Information Attack: These attacks target the electronic processes and content of the information structure through which B's decision makers observe and orient. They can directly affect B's ability and effectiveness in perceiving the situation. While PSYOP and deception operations have to pass through the sensors, information attacks do not. They can directly attack the electronic observation and orientation processes with the potential of inserting PSYOP and deception messages, disrupting or even destroying these processes. Moreover, information attacks may also have effects which cascade back into the physical domain (Waltz 6).

5. Advantages Gained Through Information Superiority

In the model above, both sides are trying to gain advantage over the opponent. The word "advantage" suggests that one side has a favorable situation relative to an antagonist. Considering the dynamic nature of engagements between two countries, the sides in a conflict try to increase their advantages compared to their adversary and to make them lasting enough to influence the other side's decisions. Age-old advantages of a fast tempo, gaining and maintaining momentum and initiative still occupy an important place in campaign planners' work, but six other types of advantages related to information superiority can help one side gain an edge over the other (Hall 61):

a. Decision Making Advantage

This is probably the most important of the six and provides a capability to seek and find other types of advantage. The goal of A in a conflict is to make more timely

and better decisions than the opponent, which will turn into efficient actions to affect B's perception and capabilities. Sustainment of this action over time will most probably cause A to end the engagement in its favor (Hall 61).

b. Intellectual Advantage

This advantage is about how one side thinks and plans compared to the other side. It is related to an ever-expanding ability to think (what to and how to think), training and education to improve thought processes; technology to better handle, process information and knowledge; access to information and knowledge relevant to the issue at hand through collaboration or a website, etc. In our scenario, the side which can develop its capabilities to think, learn, innovate, create, change, and adapt, and to develop and use readily available information technology to find information and knowledge will have a better chance to sustain this advantage over time. This advantage allows better plans and decisions, which will be more effective in influencing the adversary when turned into action (Hall 61).

c. Knowledge Management Advantage

"Knowledge management is the purposeful and systematic retrieval, processing, organizing, analyzing, synthesizing, and sharing of data, information, and knowledge among knowledge workers, decision makers, and organizations" (Hall 62). If A gains this advantage, it will be able to use knowledge as a lever for gaining entry into the mental domains of knowing, understanding, deciding, and acting. Given that both sides are evenly matched, this advantage will make A's actions more effective and help A gain edge over B (Hall 62).

d. Technology Advantage

Technology advantage can help A make better decisions than B and provide a means to achieve superior maneuverability which makes positional advantage possible. It can also provide both sides the means for better self protection. Killing and destroying with more precision than the past can allow A to degrade B's capability to act faster and easier. Technology also makes faster, clearer, and more effective communication possible (Hall 62).

e. Positional Advantage

In the conventional military sense, positional advantage enables one side to seize the initiative, control the tempo of an operation, and seize and sustain momentum. In the traditional perspective, holding the high ground or a key bridge, etc. gives one side positional advantage. In a nontraditional perspective, positional advantage might mean that one side gains advantage along avenues of approach by gaining a positional advantage in the cyberspace. Key terrains in this perspective could be switches, routers, databases, modems, etc. A may gain positional advantage over B by emplacing a logic bomb in B's database system, ready to inject bad code into the system (Hall 62).

f. Action Advantage

Action is the release of energy which causes effects. A can cause latent energy to come forth through its actions. Its actions will create effects which will create advantage (Hall 63).

Information superiority is dynamic; it fluctuates throughout the engagement. All sides strive to secure the advantages of information security and to deny them to their adversaries. This two-sided effort of seeking and denying advantages of information superiority is classified as offensive and defensive IO in the current doctrine:

6. Offensive Information Operations

"Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives" (Joint Publication 3-13 viii). The goal is to control the information environment. Offensive operations are designed to *limit*, *degrade*, *disrupt*, or *destroy* adversary information capabilities. The success depends on having an understanding of the opponent's information capabilities (Air Force Doctrine Document 2-5 9). Offensive IO activities include, but are not limited to, operations security (OPSEC), psychological operations, military deception, electronic warfare (EW), physical attack/destruction, and special information operations (SIO). They may also include computer network attack. Variety of situations and circumstances across the range of military operations may call for Offensive IO. With early engagement, they may have their greatest impact in peace and the initial stages of a crisis. Offensive IO can be a

critical force enabler for the Joint Force Commander beyond the threshold of crisis. Offensive IO may take place at all levels of war throughout the battlespace (Joint Publication 3-13 viii).

7. Defensive Information Operations

"Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems" (Joint Publication 3-13 viii). They are carried out through information assurance, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence, EW, and SIO. Ensuring timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes is the main goal of defensive IO (Joint Publication 3-13 viii). The defensive aspect of IO, much like strategic air defense, must always be operative. Conversely, the offensive IO, is primarily conducted during times of crises or conflicts (Air Force Doctrine Document 2-5 i). Offensive IO can also further defensive IO. Defensive IO ensure the necessary protection of information and information systems upon which joint forces depend to conduct operations (Joint Publication 3-13 viii).

D. A CAPABILITY BASED APPROACH

The new Department of Defense Directive 3600.1, which had not been released at the time of completion of this thesis, identifies only five core capabilities for IO (See Table 1). Psychological operations, military deception, and operations security capabilities influence the adversary decision-makers or groups and protect friendly counterparts. Electronic Warfare and Computer Network Operations capabilities influence or defend the electromagnetic spectrum, information systems, and information that support decision-makers, weapon systems, command and control, and automated responses. Computer Network Operations is comprised of Computer Network Defense and Computer Network Attack. IO supporting capabilities are counterintelligence, physical (i.e., kinetic) attack, physical security, and information assurance. These capabilities can have influence on decision-makers or groups or target information systems while detecting, safeguarding, and mitigating threats to friendly information systems and decision-making processes. Public Affairs and Civil-Military Operations become related IO capabilities and help shape the information environment (Harley).

IO CORE CAPABILITIES	
Psychological Operations	Military Deception
Operations Security	Electronic Warfare
Computer Network Operations	
IO Supporting Capabilities	
Counter-Intelligence	Physical Attack
Physical Security	Information Assurance
IO Related Capabilities	
Public Affairs	Civil Affairs

Table 1 IO Capabilities (After Harley)

E. A BASIC IO MODEL

Figure 2 expands the basic model introduced previously (Waltz 28). It includes feedback mechanism between opposing OODA cycles and illustrates the extension of IO to the society, authority, and media. This study will utilize both models to classify IO systems and to illustrate what parts of the system they affect. IO can also be directed towards National Information Infrastructure (NII), comprised of the society (population, private sector interests, economies), command authorities (political infrastructure, public sector), and media, while IO against the Defense Information Infrastructure (DII) continues. The IO against both NII and DII influence the OODA loop as well as the national objective of the "decide" element of the loop.

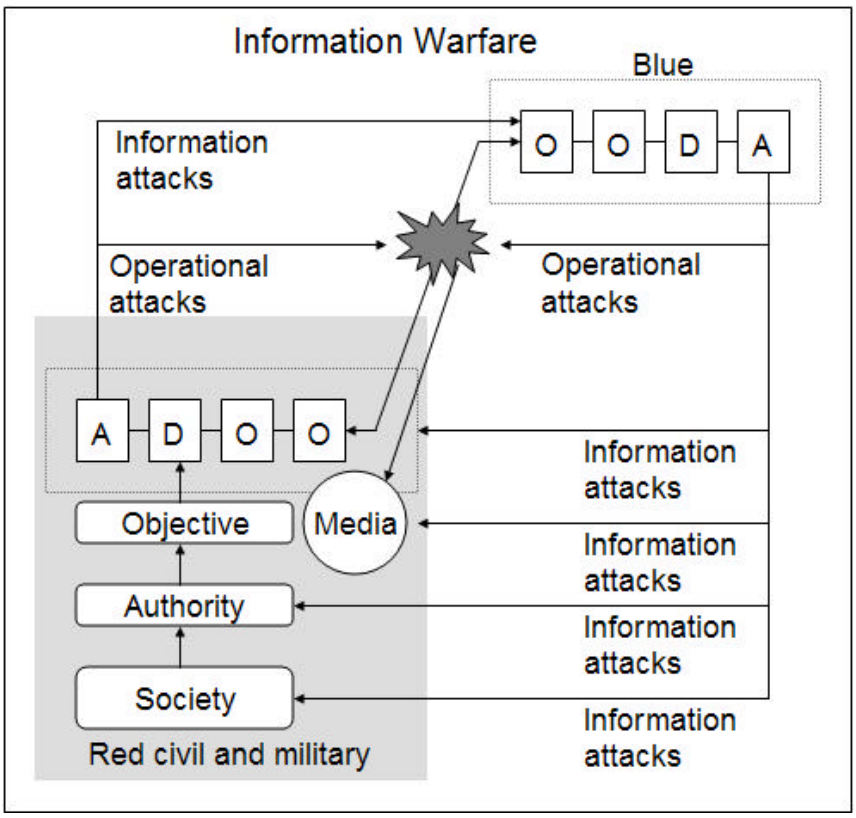

Figure 2. Expanded Model of Information Warfare with Feedback (From Waltz 28)

F. STRUCTURE OF THE STUDY

The first chapter of this thesis established a basic level of understanding of IO and introduced a few models regarding its use. The next three chapters will focus on different levels of war -- strategic, operational, and tactical, respectively -- and the use of IO at those levels. These chapters will first identify components, actors, targets, and objectives of IO at their respective levels and identify IO systems available for each level in order to provide a clear understanding. Capabilities and the models mentioned above will be the basis for this part of the study. Then these chapters will look into past examples of how these systems were utilized. Chapter V will focus on integration of different level of IO in order to achieve the best results. Finally, the thesis will conclude with emphasizing the benefits of a balanced systematic approach to military information operations and suggest further areas of research.

II. INFORMATION OPERATIONS IN THE STRATEGIC LEVEL OF WAR

A. LEVELS OF WAR IN GENERAL

The levels of war help clarify the links between strategic objectives and tactical actions. While there are no clear limits or boundaries between them, a three level system has prevailed: strategic, operational, and tactical. Types of equipment, size of units, or levels of command are not associated with a particular level. However, actions can be defined as belonging to a certain level based on their effect or contribution to achieving strategic, operational, or tactical objectives. Due to advances in technology, the compression of time-space relationships and the information age media reporting, there is a growing interrelation between the levels of war. Commanders have to be aware that in the age of constant, immediate communications, any event may cut across all three levels. Nevertheless, these levels help commanders understand the logical flow of operations in order to allocate resources and assign tasks to appropriate commands (Joint Publication 3-0 II-2). The strategic level usually concerns the President, the Secretary of Defense, and the highest military commanders; the operational level usually concerns theater commanders; and the tactical level usually concerns subtheater commanders ("Three Levels of War" 13). This chapter will briefly discuss the strategic level of war and the strategic level of IO. It will focus on the specific desired effects of this level and identify sample systems available to cause those effects.

B. IO IN STRATEGIC LEVEL OF WAR

1. Strategic Level of War

The focus of the strategic level is defining and supporting national policy, and this level relates directly to the outcome of a war or other conflict as a whole. Usually, this is the level at which modern wars and conflicts are won or lost. It "involves a strategic concept, plans for preparing all national instruments of power for war or conflict, practical guidance for preparing the armed forces, and leadership of the armed forces to achieve strategic objectives" ("Three Levels of War" 14). Strategy, on the other hand, is "the art and science of developing and employing armed forces and other instruments of national power in a synchronized and integrated fashion to secure national or

multinational objectives" (Joint Publication 3-0 II-2). The Secretary of Defense translates policy into national strategic military objectives which facilitate theater strategic planning. Susceptible enemy centers of gravity should be affected in order to impose one nation's will on another while one's own centers of gravity should be protected. Clausewitz defines the center of gravity as "the hub of all power and movement, on which everything depends" ("Three Levels of War" 14). Although the center of gravity has historically been the greatest concentration of his combat forces, contemporary use of the term includes the enemy's economy and industrial capability to wage war, will (governmental and popular), and alliances. National security strategy integrates the political, economic, informational, and military instruments of power. National military strategy is the translation of policy objectives into strategic military objectives (ends) that can be achieved by using military resources (means) and concepts (ways) such as forward basing, forward deployment, and collective security. Theater commanders may also need to develop theater military strategies to implement the national military strategy depending on the complexity of the situation and the guidance of the NCA. Strategic military objectives should be determined in such a way that, once gained, they create the conditions necessary to achieve the political purpose. To do this, military strategy should include subordinate military objectives that will create the conditions necessary to achieve the strategic objectives and thereby contribute to attaining political objectives. Thus, military strategy should ensure a clear and logical connection between ends and means ("Three Levels of War" 15).

2. Strategic Level IO

Possible IO objectives at the strategic level could be deterring war, affecting infrastructures, supporting peace operations, disrupting WMD program, etc. At this level of war IO is directed by the President and planned in coordination with other agencies and organizations outside the Department of Defense. If this includes IO conducted within a combatant commander's AOR, such operations must be coordinated with the respective combatant commander to ensure unity of effort and to prevent conflict with ongoing operational level IO. The goal of IO at this level is to engage adversary or potential adversary leadership to deter crisis and to end hostilities once they occur. IO can have widespread potential effects or may target a narrow range of adversary capabilities.

All elements of an adversary's national power (political, military, economic, informational) are possible targets. Effective use of IO at the strategic level may have the effect of minimizing potentially devastating social, economic, and political effects which would occur normally with the initiation of a military conflict. Therefore, increasing probability of mid and low intensity conflicts increase the importance of IO in the post Cold-war era. A combatant or subordinate commander within an assigned AOR may face the task of conducting specific IO in support of strategic security objectives as a result of direction by the NCA. Then the commander is responsible for integrating these IO with any ongoing offensive or defensive IO at the strategic or operational levels being planned and/or conducted in his AOR (Joint Publication 3-13 II-10).

C. SPECIFIC EFFECTS OF IO

Desired effects of IO vary depending on the circumstances. For example, the IO campaign against a country exploiting WMD will be different from the campaign against a country supporting terrorism. Air Force Doctrine Document 2-5 mentions examples of specific effects IO can achieve at this level (28). Below is an extended version of those effects for which this study will identify systems available:

- Increase situational awareness: At this level intelligence collection on adversary's current and future status, behavior, and intentions become important. The international community and other related foreign nations must also be paid attention to.
- Influence both friendly and adversary behavior conducive toward achieving national objectives through the promotion of durable relationships and partnerships with friendly nations.
- Terminate adversary leadership resistance against national objectives by affecting willpower, resolve, or confidence.
- Create a lack of confidence in an adversary's military, diplomatic, or economic ability to achieve its goals or defeat national goals.
- Incapacitate an adversary's ability to lead due to lack of communication with its forces or understanding of the operating environment.

- Deter aggression, support counterproliferation of weapons of mass destruction, and support counterterrorism.
- Win the hearts and minds of people.

This list of specific effects is nowhere near being complete, nor does this author claim that it applies to every situation. However, it just represents a sample of what effects IO is expected to achieve at the strategic level of war.

D. TARGETS / AUDIENCES OF INTEREST

The definition of three terms deserve mentioning here in order to understand the information environment: ***Global Information Infrastructure (GII)*** is the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites and satellite ground stations, fiber-optic transmission lines, networks of all types, televisions, monitors, and much more. The GII includes not only the physical facilities used to store, process, and display information, but also the friendly and adversary personnel who make decisions and handle the transmitted information. ***National Information Infrastructure (NII)*** is similar in nature and purpose to the GII and includes all government and civilian information infrastructure controlled by a state (Joint Publication 3-13 I-13). The US President's Commission on Critical Infrastructure Protection has identified the critical infrastructures under the following five sectors ("Critical Foundations: Protecting America's Infrastructures" A-1):

- Information and Communications
- Banking and Finance
- Energy (including electrical power, oil and gas)
- Physical Distribution
- Vital Human Services (See Table 2 for a detailed analysis of these sectors)

Critical Infrastructure Category	Major Infrastructure Elements	Interdependencies on Category 1 Information Infrastructure Elements
Information and Communications	Telecommunications (e.g., PTN) Computer Networks (e.g., Internet) Media Services	_
Banking and Finance	Stock and Financial Markets Commodities Market Banking and credit Investment institutions Exchange boards, trading houses, reserve systems	Electronic Commerce Networks Electronic financial transaction nets Financial record storage
Energy	Raw material resources Coal mining, processing Gas production Oil refining Resources storage (coal, oil, gas) Electrical power production Nuclear power production Electrical distribution	Production monitor and control (energy management system [EMS]) Storage monitoring Status and emergency alerting
Physical Distribution	Water supply Sewage removal, treatment Oil and gas pipeline distribution Highways, rail lines Airport and airways Mass transit	Process monitor and control (supervisory control and data acquisition [SCADA]) Power distribution monitor and control Pipeline monitor and control
Vital Human Services	Basic government operations Executive leadership Legislative leadership Judicial activities National security Emergency services Education Health care Transportation Environmental monitor/protect Public safety (law enforcement)	Telecommunication and computer networking for data and information collection, reporting, management, and control Data storage for archive of records Delivery of information and physical services

Table 2 Five Sectors of the National Critical Infrastructure Identified by the US PCCIP (From Waltz 179)

Defense Information Infrastructure (DII) is embedded within and deeply integrated into the NII. Their seamless relationship makes distinguishing between them difficult. "The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information-processing and transport needs of DOD users across the range of military operations" (Waltz 187).

The goal of IO at the strategic level is to ensure that hostilities do not mount up to IW. Therefore, at the strategic level of IO, the GII and NII are more appropriate targets compared to the DII. Possible targets in the GII could be the UN, nations friendly to the

target nation, NGOs, global media organizations, collective security organizations, allies, etc. Country A in the basic model would shape its efforts against these entities aiming to make them favor its objectives against country B. On the other hand, A could target any of the above elements of NII or all the instruments of B's national power depending on the effect it is trying to create. The focus will be on creating the certain effects which in turn will cause the decision-makers to act in accordance with A's interests. At the strategic level, though, DII would generally not be the direct target, however, A might continue to create lack of confidence in B's defense forces, to conduct Intelligence, Surveillance, and Reconnaissance (ISR) activities, and to prevent B from doing the same.

E. ACTORS / FORCES INVOLVED

As mentioned before, the President is responsible for producing national security policy and coordinating IO efforts of different agencies including DOD. A combatant or subordinate commander may face the task of conducting specific IO in support of strategic security objectives as a result of direction by the NCA. Special forces units are the most involved while other units and capabilities of the armed forces are infrequently used (i.e., UAVs, satellites, CSGs, etc.).

F. CAPABILITIES AVAILABLE

This part of the study will utilize the capabilities framework mentioned in Chapter I under the capabilities based approach to IO. As the notional IO engagement timeline in Figure 3 depicts, the strategic level of IO does not focus on the more physical part of IO (Physical and Electronic Attacks), but it does not mean that these will not take place at this level. This study will approach the strategic level as the period before hostilities mount to armed conflict and will follow its soft power applications into the period during and after conflict. IO must be planned and applied in every phase of any hostility situation in order to achieve the most efficiency.

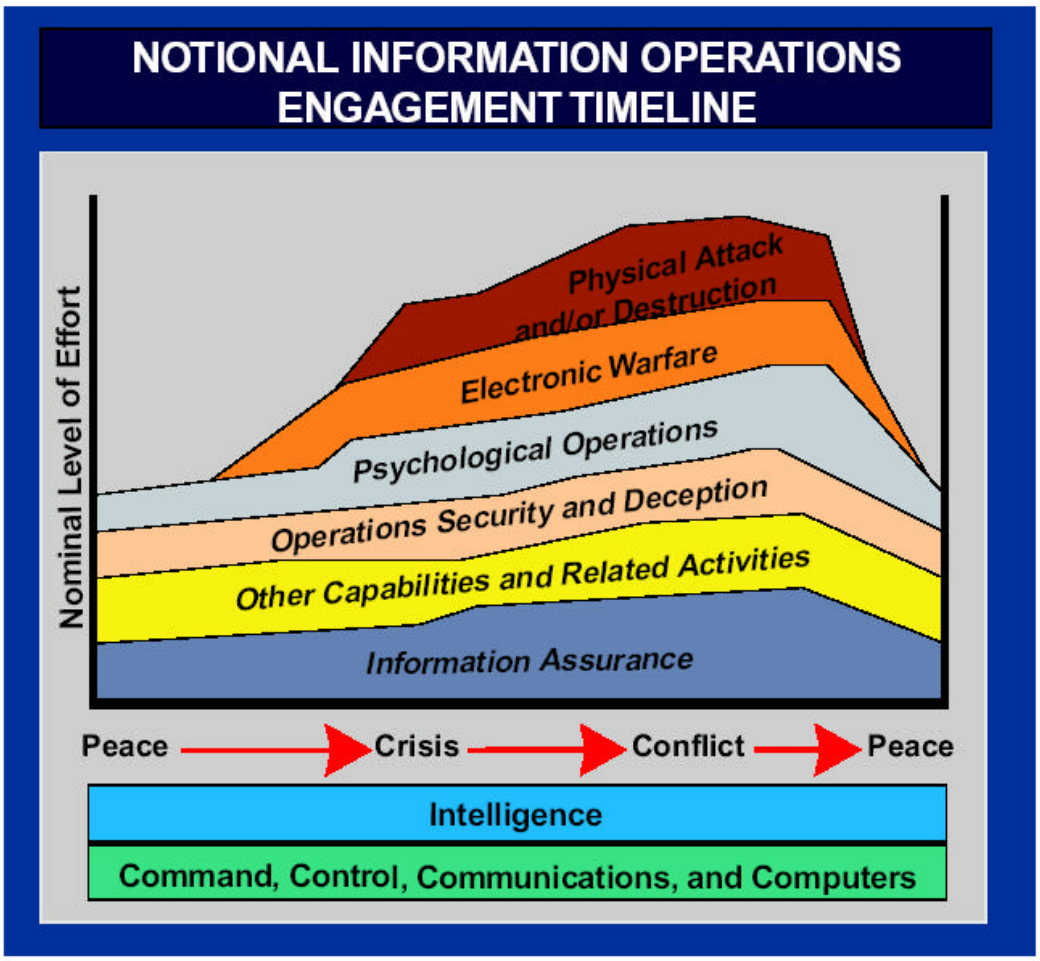

Figure 3. Notional IO Engagement Timeline (From Joint Publication 3-13 II-8)

1. IO Core Capabilities

Psychological Operations: PSYOP are actions that convey selected information and indicators to foreign audiences with the intention of influencing emotions, motives, reasoning, and eventually the behavior of foreign governments, organizations, groups and individuals. At the strategic level, it may take the form of political or diplomatic positions, announcements, or communiqués (Joint Publication 3-13 II-4). Since PSYOP have a bad reputation, it is usually more appropriate not to utilize such activities branded as PSYOP. Public diplomacy and public affairs should be prominent. These should inform the target audiences (including own public) of the NCA's policies while other acts of perception management can be applied in different ways (Joint Publication 3-61 III-18). Arquilla and Ronfeldt argue that the US grand strategy of openness versus Soviet Union's suppression of truth played an important role in the final US victory of the Cold

War. However, a "guarded openness" might be a better strategy to increase the deterrent capability of the US (ultimate goal of IO at the strategic level of war) in the current world order (Arquilla and Ronfeldt 432). With Public Affairs and Diplomacy in the front line, perception management actions not branded as PSYOP can be instrumental in achieving the desired effects.

Military Deception: Military deception is focused on desired behavior rather than just misleading thinking. The goal is to cause the adversary decision-makers to form inaccurate impressions about friendly force capabilities and intentions, to misappropriate their ISR assets, and to ineffectively position their combat and combat support units. Conducted effectively, deception can easily multiply the effects of the operations, bringing a quicker end to the hostilities. Since deception is a top-down process, its integration into the strategic level IO planning is critical. At this level it might equate to creating a favorable perception of friendly forces, capabilities, dispositions, and intentions in the mind of the adversary. In the analogy of a chess game, deception covers the movement of the pieces. When the opponent realizes how the pieces are set up on the board, it is too late for him to win the game. Similarly deception is the art of placing capabilities unnoticed by the adversary, so that when the adversary decision-makers realize the situation, they perceive the desperateness of their chance of success. To achieve such an effect, intelligence operations are critical and resources must be committed to make deception believable (Joint Publication 3-13 II-4). Beware that deception may also backfire, especially if it is perceived as a common practice. At the strategic level such a perception may cause the loss of credibility.

Operations Security (OPSEC): The purpose of OPSEC is to slow the adversary's decision cycle during friendly operations, which provides easier and quicker attainment of friendly objectives. OPSEC denies the adversary the critical information about friendly capabilities and intentions and tries to blind the adversary forcing it to react as best as its guess on friendly actions. OPSEC requires the knowledge of how capable the opponent is in collecting intelligence. Integration of OPSEC with other capabilities shapes the adversary's perception on friendly operations to friendly advantage. What differentiates OPSEC from pure defensive IO is that OPSEC is integrated into offensive IO so that the adversary cannot realize what is about to happen

and respond accordingly in a timely manner. Early integration of OPSEC into mission planning is paramount in friendly operations' achieving the desired effects without facing an effective response from the adversary (Joint Publication 3-13 II-3). Since wars can be won or lost at this level, OPSEC becomes critical for IO's success at the strategic level. Also the fact that military is not the dominant instrument of power at this level requires a sense of covertness in certain actions, so that hostilities do not escalate without control. The covertness of actions also makes OPSEC a key element of success at this level. The ability to block adversary's avenues of collecting ISR or flooding them with deceptive information (integrated with military deception) becomes important at this level.

Electronic Warfare (EW): EW encompasses any military action which uses electromagnetic and directed energy weapons to control the electromagnetic spectrum or to attack the enemy. It is divided into Electronic Attack (EA), Electronic Protection (EP), and Electronic Support (ES). EA intends to degrade, to neutralize, or to destroy adversary combat capability in the electromagnetic spectrum. EP aims to protect friendly use of electromagnetic spectrum by minimizing the effects of friendly or adversary EW. ES detects, identifies, and locates sources of intentional or unintentional radiated electromagnetic energy in order to improve situational and threat awareness. Use of EA should be conducted with respect to well-established principles, and it must be understood that EA might cause escalation of hostilities at the strategic level (Joint Publication 3-13 II-5).

Computer Network Operations: Computer Network Operations (CNO) consists of Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA). CND and CNA are defined as:

> **Computer Network Attack:** Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA. Also called CNA.

> **Computer Network Defense:** Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called CND (Joint Publication 1-02 110).

Besides the regular avenues of approach, through the World Wide Web and the Internet, the physical destruction of a computer system or network by kinetic means also qualifies as CNA. If a computer is not connected to a network or the Internet and is a stand-alone system, then it will either have to be physically destroyed or have malicious computer code physically inserted into its software program. It is the ability to disable an adversary's computer system from afar, often from a safe location, which makes CNA desirable. Another facet of the big four "D" word missions -- disrupt, deny, degrade, and destroy -- is actually gaining access to a computer, which is often referred to as Computer Network Exploitation (CNE). CNE is usually the hardest part of CNA. Getting past the security systems and gaining access is definitely tricky. Legal, political, and technological constraints have kept CNA from being fully exploited as envisioned, and these must be considered before its use (Joint Command, Control and Information Warfare School 64). At the strategic level, CNO can prove to be very useful in intelligence collection, counterintelligence operations, slowing enemy decision cycle, infrastructure targeting, etc. depending on the level of technological sophistication of the adversary.

2. IO Supporting Capabilities

Counterintelligence: Counterintelligence protects operations, information, systems, technology, facilities, personnel, and other resources from espionage, sabotage, or terrorist activities by foreign intelligence services, terrorists groups, and other elements. Counterintelligence threat estimates and vulnerability assessments identify potentially exploitable friendly information weaknesses and vulnerabilities (Air Force Doctrine Document 2-5 18). This capability is an important part of defensive IO since it prevents the adversary from gaining decision-making advantage through relevant, timely, and accurate information about friendly capabilities and intentions.

Physical Attack: Physical attack refers to the use of "hard kill" weapons against designated targets, and could serve as a key element in an integrated IO effort (Joint Publication 3-13 II-5).

Physical Security: "That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft" (Joint Publication 1-02 407).

Information Assurance (IA): "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (Joint Publication 1-02 254). IA protects information systems against unauthorized access or information corruption. It involves computer security, communications security, and the measures necessary to detect, document, and counter such threats. *Computer security* involves the measures and controls, such as policies, procedures, and the hardware and software tools necessary to protect computer systems and information *Communications security* includes measures and controls such as cryptosecurity, transmission security, emission security, and physical security of communications security materials and information (Air Force Document 2-5 17).

3. IO Related Capabilities

Public Affairs (PA) : PA mission is to expedite the flow of accurate and timely information to internal (own organization) and external (the public) audiences. PA activities create an awareness of the military goals during a campaign or operation and inform internal and external audiences of significant developments affecting them. A JFC can inform an adversary or a potential adversary about the friendly force's intent and capability through the public media. PA activities should not be used as a military deception capability or to provide disinformation to either internal or external audiences since this will reduce its credibility (Joint Publication 3-13 II-6).

Civil Affairs (CA): CA activities help military commanders establish and maintain relationships between their forces and the civil authorities and general populations, resources, and institutions in friendly, neutral, or hostile areas where their forces are employed. CA may take place before, during, subsequent to, or in the absence of other military operations. CA activities strengthen the capabilities of a host nation in

effectively applying its indigenous resources to mitigate or resolve its instability, privation, or unrest and in this way support the JFC's initiatives to improve relations with friendly foreign military forces and civilian populations and regional strategy and long-term goals. CA and PSYOP mutually support each other within civil-military operations (CMO) (Joint Publication 3-13 II-6).

G. EXAMPLES OF IO APPLICATION

This section will focus on how the systems of above capabilities relate to the desired effects stated above:

Increase situational awareness: At this level intelligence collection on the adversary's current and future status, behavior, and intentions become important. The international community and other related foreign nations must also be paid attention to. Well-informed decisions will always bring about the best results. They are more important at the strategic level since this is the level in which wars can start or end. ISR capabilities help NCA and top-level decision-makers in understanding the international and adversary situation. There are several other agencies which also deal with intelligence, and all intelligence gathering efforts should be combined in order to achieve the best awareness. See Table 3 for the major categories of intelligence. Several sensor systems can help in achieving a better situational awareness. Space systems like geostationary or polar orbital satellites can provide broad area search and precision imaging while some others can detect missiles and nuclear activity. UAVs and systems like U2 can also provide a whole range of intelligence with their multitude of sensors. ES can also be useful in detection of communications in and around the target country. EC-130E Compass Call can be utilized if airspace is available.

Influence both friendly and adversarial behavior conducive toward achieving national objectives through the promotion of durable relationships and partnerships with friendly nations: Public affairs, diplomacy, and psychological operations are critical in achieving this effect. The systems and links which make open communications and media can be seen as the enabler of public affairs and diplomacy. PSYOP also uses some of the same systems and more in order to get its message through. TV and communication satellites, radio broadcast transmitters, telephone lines, Internet / e-mail,

cellular networks, and written media are a few samples of those systems and links. PSYOP at the strategic level may also use systems like EC-130E Commando Solo aircraft for custom radio and TV broadcast. It may even use motion pictures by the film industry to get the desired message across.

Source Type	Intelligence Category	Representative Sources
Open sources: Human and technical means	OSINT: Open source intelligence	Foreign radio and television news sources Foreign printed materials: books, magazines, periodicals, journals Diplomatic and attaché reporting Shortwave radio, telecomm, Internet conversations Foreign network computer sources Gray literature (printed and electronic)
Closed Sources: Human means	HUMINT: Human intelligence	Reports from agents in foreign nations Discussions with personnel in foreign nations Reports from defectors from foreign nations Messages from friendly third-party sources
Closed Source: Technical means	IMINT: Imagery intelligence	Surveillance imagery (static air and space imagery of the Earth) Surveillance imagery (terrestrial static and video imagery)
	SIGINT: Signals intelligence	ELINT electromagnetic signals monitoring (externals: events, activities, relationships, frequency of occurrence, modes, sequences, patterns, signatures; or internals: contents of messages) Moving target indications (MTI) tracking data COMINT communications traffic monitoring for externals and internals FISINT – foreign instrumentation signals intelligence (telemetry: TELINT, beacons, video links)
	NETINT: Network intelligence	Network analysis and monitoring Network message interception, traffic analysis Computer intrusion, penetration, and exploitation
	MASINT: Measurements and signals intelligence	Technically derived intelligence from all sources (parametric data) to support real-time operations (e.g., electronic support measures, combat identification, tactical intelligence analysis) MASINT exploits physical properties (nuclear, biological, chemical), emitted/reflected energy (RF, IR, shock waves, acoustics), mechanical sound, magnetic properties, motion, and materials composition

Table 3 Major Intelligence Categories (From Waltz 117)

Terminate adversary leadership resistance against national objectives by affecting willpower, resolve, or confidence: Looking back at the expanded IW model in Figure 2, three groups should be the main target: society, authority, and media. The authority and the society should be constantly reminded of friendly intentions and capabilities through public affairs and diplomacy. Media and open communications systems mentioned above will serve for this purpose. PSYOP can be used against the society in an effort to decrease their will to resist friendly intentions. Same means as above can be used for a more customized message. Modifying military units as a show of force or physically attacking certain targets may also help PSYOP campaign. Moving a

Carrier Strike Group (CSG) or using PGMs to attack certain infrastructure targets are strong messages.

Create a lack of confidence in an adversary's military, diplomatic, or economic ability to achieve its goals or defeat national goals: Using diplomacy to gain support of the international community and imposing economic sanctions will serve degrading diplomatic and economic ability. Furthermore, CNO can be utilized against the economic infrastructure which can bring chaos by disrupting economic activity. Logical bombs, viruses, or denial of service attacks may be helpful. PSYOP messages of strong friendly forces versus weaker adversary forces will also help. PSYOP can also use media to display advances in friendly military technologies. Show of force with CSGs and PGMs might also cause the desired effect.

Incapacitate an adversary's ability to lead due to lack of communication with its forces or understanding of the operating environment: EW, CNO, physical attack, military deception, OPSEC, and IA will be prominent in achieving this effect. There are several EW suites that can perform jamming of enemy forces. EC-130E Compass Call, EA-6B Prowler are just two of those. Physical attacks on command and control links and nodes with cruise missiles or JDAMs help achieve this goal. CNO can be utilized to bring down command and control networks with denial of service attacks, Trojan horses, etc. Military deception, OPSEC, and IA can help blind the adversary of the friendly disposition and intentions. Several systems helping these capabilities are stealth aircraft and vehicles, IDS, secure network servers, encrypted tactical links, special forces covert actions, etc.

Deter aggression, support counterproliferation of weapons of mass destruction, and support counterterrorism: Public diplomacy can bring about an international consensus on the illegality and unacceptability of these behaviors. Treaty regimes can increase this resolve. Utilizing open media and communication systems to communicate the strong resolve against the above evils will help reduce their occurrence. Above all PSYOP with physical action might prove to be more deterrent. Use of PGMs and special forces units are two options available.

Win the hearts and minds of people: PSYOP, PA, and CA are the prominent capabilities in winning the hearts and minds of people. Regular open media, improved with EC-130E Commando Solo broadcasts and leaflet bombs will be PSYOP systems of choice. PA will be conducted through the media and other open communication channels.

H. SUMMARY

Effective use of IO at the strategic level may minimize potentially devastating social, economic, and political effects which would occur normally with the initiation of a military conflict. The President directs the IO efforts of all related agencies in order to achieve the desired effects. While military action is generally not in the front line of strategic level IO, a theater commander might have to conduct specific operations as directed by the President. GII and NII become the main targets of IO at this level. Some low-profile operations may also be conducted towards DII. The effects desired at this level are geared towards persuading the target country to act in accordance with friendly interest without having to use military force. Nevertheless, there are certain military systems available that help achieve certain effects. Strategic level is usually the level at which the wars are won and the achieved effects cause the operational and tactical level operations to go smoother or harder. In case that hostilities require military action, the operational and tactical level IO should start where the strategic level has left off.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INFORMATION OPERATIONS IN THE OPERATIONAL LEVEL OF WAR

The levels of war are tools that clarify the links between strategic objectives and tactical actions, and there are no clear limits or boundaries between them. Therefore, the strategic level actions continue as the operational level begins. The higher level sets the conditions for the lower level. An effective strategic level IO will in turn cause operational level efforts to go smoother. Also it is not desirable to start operational IO from scratch when the military conflict begins.

A. IO IN THE OPERATIONAL LEVEL OF WAR

1. Operational Level of War

The operational level of war is the level at which major operations and campaigns are conducted and sustained to accomplish strategic objectives. The operational level is the link between tactical employment of forces and strategic objectives. This level focuses on operational art which is the use of military forces to achieve strategic goals through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles. Operational art determines when, where, and for what purpose available major forces will be employed in order to influence the adversary disposition before combat. The deployment of those forces, their commitment to or withdrawal from battle, and the arrangement of battles and major operations to achieve operational and strategic objectives are governed by operational art. Tactical commanders fight the current battle, but the operational commanders need to look deeper in time and space. They seek to shape the possibilities of upcoming events and to anticipate the results of battles and engagements so that they can exploit them (FM 3-0 2-2). A campaign in a war consists of employment of military forces in a series of related military operations to accomplish a common objective in a given time and space. A campaign in activities short of war involves a series of related military, economic, and political operations to accomplish a common objective in a given time and space ("Three Levels of War" 16). Operational art requires commanders to answer the following questions:

> What military (or related political and social) conditions must be produced in the operational area to achieve the strategic goal? (Ends)

What sequence of actions is most likely to produce that condition? (Ways)
How should the resources of the joint force be applied to accomplish that sequence of actions? (Means)
What is the likely cost or risk to the joint force in performing that sequence of actions?
What resources must be committed or actions performed to successfully execute the JFC's exit strategy? (Joint Publication 3-0 II-3)

2. Operational Level IO

The operational level is concerned with employing IO in a theater of war or theater of operations to obtain an advantage over the enemy. IO at this level involves the use of military forces to achieve strategic objectives through the design, organization, integration, and conduct of strategies, campaigns, and operations. Possible IO objectives at this level could be exposing adversary deception, isolating enemy top-level decision-makers and/or military commanders from forces, etc. The combatant commander within the assigned AOR normally conducts IO at this level of war, or he may assign that responsibility to a subordinate commander. The focus for IO at the operational level of war will be an adversary or potential adversary in the respective AOR. IO at the operational level of war can also have strategic values with their implications in opponents' perceptions (Joint Publication 3-13 II-10).

B. SPECIFIC EFFECTS OF IO

Desired effects of IO vary depending on the circumstances. For example, the IO campaign against a country exploiting WMD will be different from the campaign against a country supporting terrorism. Air Force Doctrine Document 2-5 mentions examples of specific effects the IO can achieve at the operational level of war (28). Below is a list of those effects:

- Negate an adversary's ability to strike. Incapacitate its information-intensive systems. Create confusion about the operational environment.
- Slow or cease an adversary's operational tempo. Cause hesitation, confusion, and misdirection.
- Negate an adversary's command, control, communications, computers, and intelligence capability while easing the task of the war-to-peace transition.

Using non-lethal IW techniques instead of physical attack preserves the physical integrity of the target leaving it for use later if needed or prevents great cost later to reconstruct it during the war-to-peace transition.

- Influence adversary and neutral perceptions away from adversary objectives and toward friendly objectives inducing surrender or desertion.
- Enhance friendly plans and operations by disrupting adversary plans.
- Disrupt the adversary commander's ability to focus combat power.
- Influence the adversary commander's estimate of the situation. By creating confusion and inaccuracy in the assumptions an adversary makes regarding the situation, the direction and outcome of military operations can be influenced (Air Force Doctrine Document 2-5 29).

C. TARGETS / AUDIENCES OF INTEREST

Actors of the GII (friendly or hostile nations, NGOs, collective defense organizations, UN, etc.) are usually interested in a conflict situation and receive their information through the global media, communication systems, envoys, ambassadors, etc. While GII should not be neglected, it is mostly the President's responsibility and part of the strategic level of IO. However, the global and national media with its extensive reach may cause operational and tactical level actions to have strategic influence affecting audiences in the world and the home front. Therefore, media must be perceived and treated as a critical target at this level. Nevertheless, the adversary NII and DII becomes the main target of IO at this level. As hostilities and the level of conflict rises, the DII gains prominence over NII. Several groups of targets include the adversary country's public, national level decision authority, top-level commanders, field commanders, soldiers, C4I links and nodes, economic, logistical and transportation infrastructure, etc.

D. ACTORS / FORCES INVOLVED

The theater commander has the ultimate responsibility of planning and integrating IO elements in his AOR. Military capabilities become more available and prominent at the operational level of IO. However, other agencies may continue to conduct IO and IO related activities in the AOR and in the rest of the world. A liaison system should be set

up in order to coordinate these activities to disseminate a synchronized message to the target audiences in line with the strategic guidance of the President. Any unit in the AOR can be a part of IO either directly or indirectly.

E. CAPACITIES AVAILABLE

As depicted in the notional IO engagement timeline in Figure 3, the planning and integration of harder parts of IO (in the form of EW, physical attack, or more physical versions of other capabilities) increases as a crisis develops into force on force combat. These actions might be more risky, expensive, and destructive for both sides. A good use of operational art may bring about a quicker end to the hostilities while a poor planned operational level of war may cause the hostilities to entangle time and resources of both sides. Operational level IO becomes an important force enabler in the theater commander's alternatives in achieving the strategic objectives. Following is a brief examination of IO and related capabilities at the operational level with available systems:

1. IO Core Capabilities

Psychological Operations: Since PSYOP intend to influence emotions, motives, reasoning, and eventually the behavior of foreign governments, organizations, groups and individuals, a good application of PSYOP can save a lot of friendly and adversary lives. Operational level PSYOP should start where the strategic level has finished in order to achieve consistency and effective use of resources. Joint military PSYOP objectives across the range of military operations can be seen in Figure 4. PSYOP at this level can include the distribution of leaflets, radio and television broadcasts, loudspeaker broadcasts, and other means of transmitting information that encourage enemy forces to defect, desert, flee, or surrender. PSYOP integrated into persistent attacks can have a synergistic effect accelerating the degradation of morale of enemy forces and further encouraging desertion (Joint Publication 3-13 II-4).

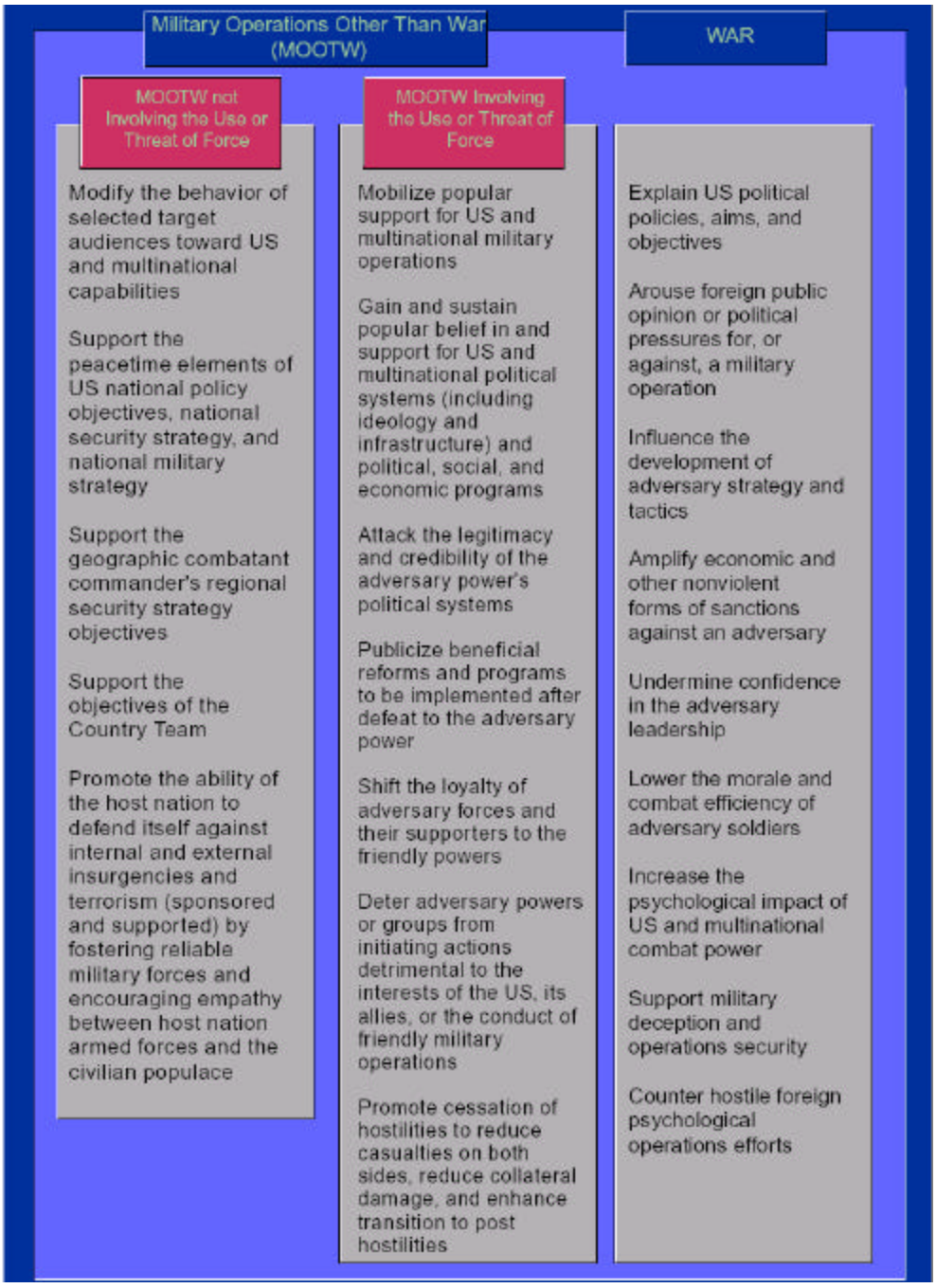

Figure 4. Joint Military PSYOP Objectives Across the Range of Military Operations (From Joint Publication 3-53 V-2)

Military Deception: The operational level of war is concerned with creating the conditions which will support the best use of available resources in the attainment of the strategic objectives. Military deception should focus on causing the adversary commander to incorrectly estimate the situation in the operational area with respect to friendly force dispositions, capabilities, vulnerabilities, and intentions. A "successful"

deception might just have to cause the adversary commander to hesitate in making decisions during a critical time in the operations. Some of the military deception goals are as follows:

- Cause the adversary commander to employ forces (including intelligence) in ways that are advantageous to the joint force.
- Cause the adversary to reveal strengths, dispositions, and future intentions.
- Overload the adversary's intelligence and analysis capability to create confusion over friendly intentions to achieve surprise.
- Condition the adversary to particular patterns of friendly behavior that can be exploited at a time chosen by the joint force.
- Cause the adversary to waste combat power with inappropriate or delayed actions (Joint Publication 3-58 II-1).

Deception should be planned at the top level and all the other operations should fit in the deception plan. The deception at the operational level should link the strategic level deception planning to the tactical level actions. Intelligence and counterintelligence operations are very important in deception operations, specifically in identifying adversary decision-makers, their perceptions on friendly forces, and adversary information gathering capabilities; in providing estimates of adversary actions under differing scenarios; in establishing and monitoring feedback channels; and penetrating adversary OPSEC measures and deceptions (Joint Publication 3-58 II-2).

Operations Security (OPSEC): OPSEC at the operational level denies the adversary the critical information about friendly capabilities and intentions and slows the adversary's decision cycle during friendly operations. OPSEC is a process which consists of five distinct actions: *identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk,* and *application of appropriate OPSEC measures*. The ultimate threat to OPSEC is the adversary commander. The intent of OPSEC as a part of IO should be to force the adversary commander to make ineffective decisions based upon insufficient information and/or to delay the decision making process due to missing information. Denial of critical information contributes to uncertainty and slows the adversary's decision cycle. Traditional OPSEC measures such as action control, countermeasures, and counteranalysis can hide critical information. The OPSEC process may identify particular adversary information collection, processing, analysis, and distribution systems. Attacking these systems can forestall the adversary commander's

ability to collect information. Counterintelligence support is a must for successful OPSEC. The news media's inevitable presence during military operations also complicates OPSEC. The capability of the news media in the operational area to transmit information on a real-time basis to a worldwide audience makes media a lucrative source of information to adversaries. The aspects of a military operation designated as "critical information" must be denied to the adversary by developing guidelines that can be used by both military and news media personnel to avoid inadvertent disclosure of that information (Joint Publication 3-54 I-3).

Electronic Warfare (EW): EW at the operational level is waged throughout the EM spectrum with the objective of securing and maintaining effective control and use of the spectrum by friendly forces and denying its use by an adversary through damage, destruction, disruption, and deception. The operational environment in which a military operation is carried out determines the need for control of the EM spectrum and the type of EW actions that can be used to control that spectrum. Depending on the threat posed by adversary forces, the reliance of adversary forces on use of the EM spectrum, and the objectives of the operation, differing type and level of EW actions suit to particular military operations. ES, on the other hand, supports decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing by providing required information. ES data can be used to produce signals intelligence (SIGINT), measurement and signature intelligence (MASINT), and provide targeting for electronic or destructive attack. SIGINT can also be used as battle damage assessment and feedback on the effect of the overall operational plan (Joint Publication 3-51 I-2).

Computer Network Operations: CNO gains more momentum at this level compared to the IO at the strategic level of war. CNA can be very effective at the operational level depending on the technical sophistication of the adversary. On the other hand, CND becomes critical when the friendly GII, NII, and DII rely heavily on information technology. CNA may target both DII and NII, or due to shared infrastructure elements, an attack for one may cause the other one also to be affected (collateral damage). In order to prepare adequately for a CNA operation, some of the following questions must be answered:

- Where is the system that is to be the target?
- What room on what floor of which building?
- What kind of hardware is hosting the system?
- What software is resident on the computer and which version is currently installed?
- Is the computer connected to the World Wide Web or is it "air-gapped," i.e., a stand-alone system? (Joint Command, Control and Information Warfare School 65)

A CNA victim computer may show no sign of the attack, it might explode, or it might just stop working. These are just results of different methods of attacks. Considering that most computer systems do not have dedicated support staff like most major weapon systems do, their malfunctions may go unfixed for a while. This time lag, even, makes CNO effective in slowing decision cycle of the adversary or in gaining intelligence with few resources. For the same attractiveness of CNA makes good CND a must (Joint Command, Control and Information Warfare School 65). Since the level of security for most NII systems is not as good as DII systems, a successful CNA against those -- especially against vital human needs related infrastructure -- can cause extremely high damages. As a result, CNO can prove to be very useful in intelligence and counterintelligence operations, slowing adversary decision cycle, infrastructure targeting, etc. depending on the technological sophistication of the adversary.

2. IO Supporting Capabilities

Counterintelligence: Counterintelligence at the operational level is also concerned with protecting operations, information, systems, technology, facilities, personnel, and other resources from espionage, sabotage, or terrorist activities by foreign intelligence services, terrorists groups, and other elements. This capability prevents the adversary to collect relevant, timely, and accurate information about friendly capabilities and intentions preventing the adversary from gaining decision-making advantage. Therefore, CI is a critical supporting capability to operational level IO.

Physical Attack: Physical attack, the use of “hard kill” weapons against designated targets, becomes an inseparable part of an integrated operational level IO effort. It can be used to attack some key targets directly, or it can be a part of perceptional level targeting as part of PSYOP or deception.

Physical Security: Since military actions become more and more common at this level of war, physical security of especially C4I systems, links, nodes, and personnel becomes critical. A good physical security helps the OPSEC effort to blind the adversary on friendly capabilities and actions.

Information Assurance (IA): The information becomes more critical for the soldiers on the ground as the hostilities turn into force-on-force conflict. Unauthorized access to information systems and information corruption can cause lives or the failure to attain objectives of campaigns. IA at the operational level is also concerned with computer security, communications security, and the measures necessary to detect, document, and counter threats against them.

3. IO Related Capabilities

Public Affairs (PA): PA activities continue to provide accurate and timely information to internal (own organization) and external (the public) audiences at the operational level. The news media, as part of the GII, portrays and offers commentary on military activities on the battlefield before, during, and after battles. This portrayal of military activities prior to hostile engagements can help to deter actual hostilities and/or build public support for inevitable hostilities. Media's coverage, by portraying the presence of friendly forces and/or multinational military forces in or en route to the operational area, can demonstrate the readiness, commitment and resolve of the involved countries to commit military forces to battle if necessary to protect national and/or multinational interests, lives, or property (Joint Publication 3-54 I-4).

Civil Affairs (CA): CA is a part of the overall CMO effort. At the operational level, CA supports the strategic CMO objectives while focusing on immediate or near-term issues such as health service infrastructure, noncombatant evacuation operations (NEOs), movement, feeding, and sheltering of dislocated civilians, police and security programs, synchronization of CMO support to tactical commanders, and integration of interagency operations with military operations. Theater commanders are responsible for allocating and distributing resources that enable subordinate commanders to execute CMO (Joint Publication 3-57 I-5).

F. EXAMPLES OF IO APPLICATION

This section will focus on how the above capabilities relate to the desired effects stated above:

Negate an adversary's ability to strike. Incapacitate its information-intensive systems. Create confusion about the operational environment: This desired effect addresses three different realms of IO targets: Physical capability, information systems, and human minds respectively. Directly targeting the physical capability with physical attacks is not the only way to negate the adversary's ability to strike efficiently. Incapacitating the information systems and creating confusion in the decision-makers' minds can also help achieve this effect. Therefore, attacking the latter two targets is preferable to force-on-force attrition type of engagements. Nevertheless, in the realm of IO, physical attack can also be improved with the help of satellite (imaging and GPS) and precision targeting (PGMs, i.e., Tomahawk missiles) systems, which can help in better target identification and overwhelmingly effective target elimination. EW can be used in attacking all three realms. Directed energy weapons such as HPM systems can be used in EA for direct attack. Information systems can be targeted with jamming systems like EA-6B Prowler aircraft. On the other hand, EP suites such as AN/SLQ-32 can help blind the adversary on friendly use of the electromagnetic spectrum. CNO can also prove to be useful in this desired effect. CNA targets the information-intensive systems which provide decision support to decision makers and control the weapons systems. For example, a denial of service attack can prevent the use of decision support systems, causing more confusion. A Trojan Horse attack to a weapon system's control computer could render that weapon useless for a while. Furthermore, CND, when conducted diligently, can prevent adversary from probing the friendly systems. IDS are used for this purpose. The confusion in the mind of the adversary commander can be increased with creative utilization of PSYOP and deception. A deception campaign that causes the adversary to concentrate his strike capability at irrelevant locations is a major source of confusion. This deception can be supported with PSYOP, too. All these and other operations should be integrated into the OPSEC process. IA and counterintelligence are also important and must be included in the defensive part of IO effort.

Slow or cease an adversary's operational tempo. Cause hesitation, confusion, and misdirection: The target realms mentioned in the above effect are also the same for slowing or ceasing an adversary's operational tempo. Physical confrontation is not as desirable as other options, but should also be integrated into the IO planning. Besides the option of physical attacks, the operational tempo of an adversary can be affected by slowing its decision-making process, severing communication between forces and commanders, or diminishing the soldiers' willingness to fight. At the perceptional level, PSYOP and deception can be used to cause hesitation, confusion, and misdirection. PSYOP can be effective in convincing the adversary personnel. The usual systems like leaflet bombs, TV and radio broadcasts by Commando Solo aircraft may prove to be useful. Cell phone text messages or e-mails directed towards key leaders might be another avenue to affect people's minds. The use of Internet should not be neglected for PSYOP messages. Depending on the use of the Internet, the demographics of the audience it reaches might vary, and this should be taken into consideration. PSYOP messages can be strengthened with physical actions and public affairs. The influence of media and the public on decision authority can be the target of these actions. Public affairs can utilize the conventional media channels (satellite TV, shortwave radio, etc.). Physical actions might be in form of show of force by CSG or well-thought bombing missions to selected targets. Well-crafted and efficiently transmitted to the target audience, PSYOP messages can affect the adversary soldiers' will to fight, which ultimately slows or ceases operational tempo. Deception can cause the adversary commanders to misunderstand the friendly capabilities, dispositions, and intentions creating hesitation, confusion, and misdirection. EW assets (i.e. RC-130 Rivet Joint aircraft) radiating from or collection of friendly jamming at certain points away from the main attack may help creating a false perception of friendly actions. These EW assets may be supported by physical actions, such as a beachhead clearing by special forces units. Any friendly activity that is perceived by the adversary decision-makers as a habit of the friendly doctrine can be presented to the adversary with an unexpected follow-on action as part of deception. OPSEC, on the other hand, denies critical information to the adversary commanders and slows their decision cycle. Counterintelligence, IA, CND, and physical security measures and systems can enhance OPSEC's effect of confusing the

adversary. CNA, EW, and physical attacks may also be used against infrastructure targets, such as command, control, and communications links and nodes. These attacks slow down the information gathering and dissemination of the adversary, or disrupt and destroy the command structure, which in turn slows or ceases the operational tempo.

Negate an adversary's command, control, communications, computers, and intelligence (C4I) capability while easing the task of the war-to-peace transition. Using non-lethal IW techniques instead of physical attack preserves the physical integrity of the target leaving it for use later if needed or prevents great cost later to reconstruct it during the war-to-peace transition. As Sun Tzu said "In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to recapture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them" (Sun Tzu III-1). The operational level of war is also concerned with the exit strategy as discussed above. IO presents a better way to end hostilities in line with the recommendations of Sun Tzu. The human factor is the most decisive one in the resolve to continue of the hostilities. Unless all resources of a nation are depleted through war, the will and determination of the people, commanders, and soldiers might still lead them to fight or to cause damages using different methods such as guerilla warfare and terrorism even if they knew that they had no chance to win. Destruction of people and property causes hostile feelings to thrive even after the conflict ends. Targeting adversary C4I capabilities instead of winning through attrition is a better exit strategy which brings about a more stable and longer lasting peace. The targets in this sense can be classified under three headings: Human factors (Commanders, decision-makers), links and nodes. PSYOP are useful in affecting perceptions of adversary decision-makers and commanders in to believing in the futility of their efforts to win the war. A further message can be that they will be responsible for the futile death of their soldiers, or that they will be judged after the end of hostilities for any further resistance. The soldiers can be convinced on the futility of their effort, the righteousness of their enemy's cause, and the advantages of not resisting, etc. These messages can be delivered using leaflets, loud speakers, cell phone and e-mail messages to the commanders, radio and TV broadcasts, etc. OPSEC and deception can cause a sense of blindness and enhance the desperation in their perception. CNO can attack the

C4I nodes and cause them to slow transfers or to cease functioning. EW and physical attack can also be used against C4I links and nodes. Decision-makers are like the brain of the body while C4I links and nodes are like the nerve system. If attacks against those are successful, the end result is the paralysis of the body. The country cannot put up a coordinated resistance, and the decision-makers surrender the country.

Influence adversary and neutral perceptions away from adversary objectives and toward friendly objectives inducing surrender or desertion: PSYOP, PA, and CA can be key to achieve this end. They must be coordinated and synchronized around a common theme in order to achieve the best results. PA should use the conventional media to disseminate the message that the friendly forces are righteous, they treat the POWs with dignity, and the recent POWs are now happier than they used to be under serving the adversary regime. PSYOP can disseminate the similar themes through the systems and methods discussed before. CA can be useful in preparing the conditions necessary for treatment of POWs with dignity. It can also be utilized to represent the friendly good will in the occupied territories by bringing the living conditions back to normal. CA must be coordinated with PSYOP and PA so that its message can get across through appropriate ways of communications.

Enhance friendly plans and operations by disrupting adversary plans: Disrupting adversary plans can be achieved in two ways: 1. Through friendly deception, the adversary perceives the situation wrong and prepares plans which are doomed for failure. 2. The friendly forces have information superiority and have a better understanding of adversary capabilities and intentions. Through friendly ISR efforts, the theater commander can get into the adversary's decision loop and act in appropriate time and space so that adversary efforts become void. The initial requirement for getting into adversary's decision cycle is superior ISR capability. Satellites provide imagery intelligence, weather and location data while communication satellites improve dissemination of information worldwide. JSTARS and AWACS are two systems which improve situational awareness immensely. UAVs with multiple sensors enhance the Common Operational Picture (COP). Laser rangers and designators teamed up with capable soldiers like special forces units can also provide valuable information. The networking of all this information provides reach back capability to gain an edge over the

adversary. The air-fueling tankers (KC-130) and UAVs can be used as network repeaters to improve the quality of service and reach of this network. OPSEC, which denies the adversary the critical information about friendly forces, must also be coordinated, so that the enemy has to make estimates which are more prone to failure. A good ISR capability provides a good understanding of what the adversary is trying to do, a good OPSEC helps blind the adversary commander, and under these conditions the theater commander can use his creativity to disrupt the adversary plans at the appropriate time and places.

Disrupt the adversary commander's ability to focus combat power: Parts of NII and DII regarding transportation and communication are the targets of this desired effect. The adversary commander must be able to communicate his units where to mass and then, those units must be transported to the planned location, so that he can focus combat power. Communication links and nodes are the primary targets of IO in this case. CNA, EA, and physical attack may prove to be useful for this effect. See above examples for available systems.

Influence the adversary commander's estimate of the situation. By creating confusion and inaccuracy in the assumptions an adversary makes regarding the situation, the direction and outcome of military operations can be influenced: As mentioned in above effects, coordinated use of PSYOP, deception, OPSEC, EP, IA, CND, and counterintelligence can cause this effect. See above examples for sample systems.

G. SUMMARY

The operational level IO picks up where the strategic level has left off. While strategic level IO efforts still continue, operational level IO deals with employing IO in a theater of war or theater of operations to obtain an advantage over the enemy. The start of the operational level of IO usually means that the strategic efforts to protect peace have failed. The focus of operational level IO, then, becomes creating advantageous conditions for friendly military operations and bringing quick end to the hostilities. The combatant commander within the assigned AOR normally conducts IO at this level of war, or he may assign that responsibility to a subordinate commander. Since this is the level which ties the tactical actions to the strategic objectives, a great deal of attention must be paid to the IO efforts at this level. The IO at the operational level, especially, can have effects at

all three levels simultaneously. These efforts will pave the way to more successful tactical actions and a quicker and smoother attainment of strategic objectives.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INFORMATION OPERATIONS IN THE TACTICAL LEVEL OF WAR

A. IO IN THE TACTICAL LEVEL OF WAR

1. Tactical Level of War

Tactics is defined as the employment of units in combat. It focuses on the ordered arrangement and maneuver of units in relation to each other and/or to the adversary seeking to use their full potential. An engagement is fought between small forces, such as individual aircraft in air-to-air combat and normally short in duration. Engagements may include a wide variety of actions in the air, in space, on and under the sea, or on land. A battle involves a set of related engagements. Battles involve larger forces such as fleets, armies, and air forces; typically last longer; and could affect the course of a campaign (Joint Publication 3-0 II-3). When engaged in nonlethal forms of military activities, the tactical level focuses on non-combat functions. These functions include logistics assistance, provision of training, and other forms of assistance. In such cases, tactics deal with the details of implementing assistance programs. These programs are extremely sensitive to the total military, political, and social environment in which the assistance is provided ("Three Levels of War" 18).

2. Tactical Level IO

Tactical level deals with the details of prosecuting engagements in the changing environment of the battlefield. Possible IO objectives at this level could be disintegrating IADS, degrading or destroying tactical command and control, etc. Smaller units conduct the tactical level of IO. As in strategic and operational IO, the focus of offensive IO at the tactical level of war is also the human element. Human focus attempts to affect the will of the adversary's military forces to resist and to deny the adversary's use of the affected populace to gain advantage. The end result of these IO is that the affected populace is kept abreast of friendly purposes and intents (Joint Publication 3-13 II-11).

B. SPECIFIC EFFECTS OF IO

- Deny, degrade, disrupt, or destroy an adversary's use of information and information systems relating to C2, intelligence, and other critical

information-based processes directly related to conducting military operations.
- Reduce the size or capability of adversary forces.
- Deny adversary knowledge of forces (Air Force Doctrine Document 2-5 29).

C. TARGETS / AUDIENCES OF INTEREST

Identifying the appropriate target audience is hard at the tactical level of IO. The intelligence effort should be concentrated on the following criteria: The proper target is one who the tactical commander can get to and who is a factor in his area of operation (AO). The commander must consider not only the hostiles, but noncombatants in his AO as well. The audiences can include enemy commanders, paramilitary commanders, staff members who advise/support key leaders, terrorist or guerrilla leaders, junior or mid-level leadership, and third party leaders who provide support to the enemy's main effort. The commanders must focus on those operational and tactical enemies whose decision cycle when attacked will produce the greatest benefit (McNeive 52). The media can cause tactical actions to have disproportionate effects, and therefore, should not be neglected. C4I links and nodes are also promising physical targets.

D. ACTORS / FORCES INVOLVED

All three levels are related to each other in the sense that the higher level dictates what will happen in the lower level. The operational level, as mentioned before, relates the strategic goals to tactical actions. Therefore, the theater commander selects the most appropriate forces or units to accomplish the operational objectives. Subtheater level commanders utilize their units to accomplish tactical objectives, achievement of which brings about the operational objective when combined with the other tactical objectives. These commanders lead military units that are in a close proximity to the adversary targets in the sense that they can affect those targets when ordered or they can be easily affected by the adversary forces. These tactical unit commanders should gain local information superiority against adversary forces, so that they can accomplish their tasks easier. The military units involved may be any military size unit equivalent of or below corps level. They may have to conduct IO in order to accomplish their goals easier or they might be tasked with specific IO missions (i.e., tactical PSYOP units, tactical EA aircraft).

E. CAPABILITIES AVAILABLE

IO, at the tactical level, should be a focused, integrated effort to control an enemy's information in a way which will directly support a commander's concept of operations. The commander must look past the physical impact he wants to achieve and must consider how he can influence the way his adversary thinks. While permanently changing the way a person thinks or acts is often a goal of strategic level IO, the commander must realize that he can only manipulate, corrupt, block, or destroy information so that the target audience will be confused, persuaded, or intimidated during a period of time of his choosing (McNeive 52).

1. IO Core Capabilities

Psychological Operations: PSYOP at the tactical level is conducted in the area assigned to a tactical commander during conflict and war to support the tactical objectives against adversary forces. It deals with the psychological dimension which affects those fighting the battle, their military leaders and staffs, the political leaders, and the local civilian population. The end result of PSYOP is to face an enemy that is both unsure about its fighting cause and capabilities, sure about its impending defeat, and even if unwilling to surrender, has little will to engage in combat (Joint Publication 3-53 I-3).

Military Deception: Military deception at the tactical level also focuses on causing the adversary commander to incorrectly estimate the situation in the battlefield with respect to friendly force dispositions, capabilities, vulnerabilities, and intentions. The goal of deception is to gain the element of surprise. Gaining surprise causes the target to be confused. His tempo slows down and is unable to make timely and accurate decisions. Afterwards, the target's removal from the situation either through death, withdrawal, or capitulation can be accomplished much easier (McNeive 52).

Operations Security (OPSEC): OPSEC maintains its critical position also at the tactical level. Tactical level OPSEC is not much different from the operational level OPSEC other than scale. It also requires the management of indicators and seeks to limit an adversary's ability to detect or derive useful information from observing friendly activities. The commander must remember that his adversaries are also reaching out to

affect targets, too. Information can leak out of every corner of a command unless strict OPSEC measures are employed and enforced (McNeive 52).

Electronic Warfare (EW): EW is an important IO tool at the tactical level with its operations spread throughout the EM spectrum. EW can perform multiple tasks with the objective of securing and maintaining effective control and use of the spectrum by friendly forces and denying use by an adversary through damage, destruction, disruption, and deception. Affecting adversary communication networks, radar and IADS systems might be a few of those important missions.

Computer Network Operations: CNO can be an effective tool for the tactical commander depending on the technological sophistication of the nearby adversary forces. However, the tedious nature of I might not make it such a quick and easy alternative in the heat of battle. However, I in the form of physical destruction of computer systems or nodes might be a feasible and efficient option. On the other hand, CND maintains its relevancy especially due to advent of wire and wireless networks in the battlefield.

2. IO Supporting Capabilities

Counterintelligence: Counterintelligence at the tactical level is also an important capability since it prevents the adversary from gaining decision-making advantage through relevant, timely, and accurate information about friendly capabilities and intentions.

Physical Attack: Physical attack is much more prominent at the tactical level of war. The commander must keep in mind that anything that can influence the way someone thinks should be considered. The planning for IO should also include those physical attacks which will produce the intended behaviors of the opposing force commander.

Physical Security: Physical security is also paramount at the tactical level of war due to the proximity to the adversary. Violation of this may cause immediate undesired results which are favorable to the adversary.

Information Assurance (IA): The tactical commander must also take the necessary steps of IA which protects friendly information systems against unauthorized

access or information corruption. Computer security, communications security, and the measures necessary to detect, document, and counter such threats are still important for achieving information superiority.

3. IO Related Capabilities

Public Affairs (PA): Though not as important as the operational level PA, tactical level PA can also be a good tool to disseminate the good will and intentions of the friendly forces. Every tactical commander must be aware that their actions recorded by the media can have important effects at all levels. PA can also enhance the CA efforts in the AO.

Civil Affairs (CA): CA activities help military commanders establish and maintain relationships between their forces and the civil authorities and general populations, resources, and institutions in friendly, neutral, or hostile areas where their forces are employed. Tactical commanders perform CMO functions in order to support the theater commander's CMO guidance and in order to accomplish their own tactical objectives. These functions are normally more narrowly focused and have more immediate effects. They may include processing and movement of dislocated civilians, local security operations, and basic health service support (Joint Publication 3-57 I-5).

F. EXAMPLES OF IO APPLICATION

Deny, degrade, disrupt, or destroy an adversary's use of information and information systems relating to C2, intelligence, and other critical information-based processes directly related to conducting military operations. The IO supporting the achievement of this effect is local and mission specific. The initial requirement, though, is collection of intelligence about targets (information systems, information-based processes, commanders, and human processors of information). The tactical commander should use available ISR collection systems in order to have a better understanding of the above targets. An AN/PPS-5 combat surveillance radar or a thermal imaging system might be a few readily available systems. RQ-1A Predator type UAV and many other systems might be available at higher levels. These systems must be utilized to their fullest capabilities in order to achieve a clearer understanding of the situation. Data provided by meteorological or GPS satellites also provide invaluable information. Networking of the

friendly and adversary intelligence through wire, wireless, and satellite communication networks will help achieve a COP throughout the units in the AO. This COP can also be enhanced with higher level available intelligence. The efficient dissemination and display of this COP might be another step to improve information superiority. A sample tactical objective might be disintegrating enemy IADS. Then, EW, CNO, physical attack and OPSEC might be the proper capabilities to employ. EW systems like EA-6B can jam enemy radars while CNA might be used to generate false targets in the targeting systems. Physical attacks can destroy air defense radars and communication links/nodes between them. OPSEC in protecting the counter IADS efforts and the ongoing air missions is also another critical factor for the success of this effect. Another sample tactical objective could be degrading or destroying enemy tactical command and control. In this case, the tactical commander could utilize any of the core IO capabilities depending on their availability and suitability to his overall plan. Deception supported by PSYOP and OPSEC improving its credibility and secrecy can create surprise. Physical attack systems like close air support by F-15 aircrafts may be used to channel adversary thought processes into a certain area. PSYOP can use loudspeakers, cell phones, or enemy communication channels to persuade the enemy soldiers to drop their weapons and to surrender. EW can be used in order to jam communication links with EC-130E Compass Call while physical attack systems like JDAM can be used to destroy command and communications nodes. The commander has to analyze the situation and resources available to him in order to plan a coherent IO in support of his tactical objective.

Reduce the size or capability of adversary forces. Pure physical attack is the first option that comes to the mind, but it is inferior to the other alternatives provided by an integrated IO effort, even at the tactical level. In order to attack the human element, PSYOP can be used with the support of PA and CA. PSYOP can disseminate surrender instructions and discourage/disrupt enemy operations. At the close combat range, loudspeakers might be the system of choice. The CA activities can also be broadcasted through PSYOP. PA is also another tool to disseminate the overall message through conventional media channels. These efforts can degrade enemy soldiers' will to fight and encourage surrenders, which is a better way to reduce adversary force size. Deception and OPSEC would also help reduce the adversary capabilities by causing the opposing

commander to use them inefficiently. OPSEC tries to limit an adversary's ability to detect or derive useful information from observing friendly activities while deception seeks to create or increase the likelihood of detection of certain indicators to lead the adversary into reaching an incorrect conclusion. Information value added physical attack may also be another effective alternative. The improvement comes from friendly capabilities to detect, identify, and target from a further distance and to engage the target precisely. This is another display of information superiority and improves friendly attack efficiency extremely. JDAMs illuminated by a special forces soldier's laser designator is just one example of these systems. It must be kept in mind that these attacks may lead to an attrition battle unless friendly capabilities are clearly better than that of the adversary's. EW, CNO, and physical attacks can be used to attack the adversary's C4I links and nodes. These attacks can disrupt or destroy command and control transmission from the commander to the forces. The end result is either paralysis of the adversary force or the degradation of the command process. Lack or disruption of command and control causes an inefficient use of the adversary capabilities, supporting the desired effect.

Deny adversary knowledge of forces. Strong attention to defensive IO not only protects the tactical commander's plan from the adversary but also keeps his information flow intact. Failure to leverage information for defensive and offensive purposes can leave the commander open to exploitation (McNeive 53). Deception and OPSEC combined together, as described above, is a good way to cover indicators that reveal friendly activities while showcasing indicators that cause the adversary to reach incorrect conclusions. PSYOP can be added to the mix in order to increase the credibility of the deception scheme. Defensive IO also becomes paramount considering the proximity of adversary effects to friendly forces and capabilities. Physical security of information and information systems is critical. Cover and concealment against adversary sensors and physical attacks must be considered. Counterintelligence also becomes important since the adversary will constantly probe the friendly actions, units, and information systems with his ISR sources. The proximity allows multiple sensors to be effective. EP might be employed against adversary ES and EA systems. AN/SLQ-32 EW suite might be one alternative in EP. CND measures like IDS must be employed in order to prevent unauthorized access to the information and information systems. These measures must be

hardened with IA efforts. For example, a Tactical Operations Center's network must be free of any unauthorized physical or remote access. Physical security of the network must be improved by an IDS which monitors remote access to the network. Password and encryption protection are a few methods used for IA and can help improve the availability, integrity, authentication, confidentiality, and nonrepudiation of the friendly information. Communications security part of IA must employ cryptosecurity, transmission security, emission security, and physical security of communications security materials and information so that the adversary efforts to collect intelligence of friendly communications are averted.

G. SUMMARY

IO is a powerful force multiplier and can save a lot of friendly and enemy lives especially when the hostilities require the tactical level units to face each other in deadly combat. Therefore, the tactical level of IO is extremely important. It causes the tactical actions to be more effective, quick, and less damaging to both sides. Tactical level actions are the means to achieve the strategic level objectives employed by the operational level planning. IO must continue at all three levels for a coherent and effective use. Commanders at all levels must understand that their actions related to IO can have effects at all three levels of war.

V. INTEGRATION OF IO EFFORTS AT ALL LEVELS OF WAR

A. WHY INTEGRATE?

Previous three chapters illustrated how IO related to the strategic, operational, and tactical levels of warfare. As mentioned in the previous discussion, the concept of levels is a way to better understand the logical flow of operations in order to allocate resources and to assign tasks to appropriate commands. It is also a fact that the boundaries between the three levels are blurring as actions in one level can have implications for another one. Due to these unclear boundaries, decision-makers and commanders at all levels must be aware of the bigger and smaller pictures. In a conflict situation, the side that can best integrate the efforts in all three levels gains an advantage over its adversary by producing better strategic goals, using the operational art to find appropriate ways and means to accomplish them, and translating the strategic goals into tactical actions.

The aforementioned importance of IO for the present state of warfare makes integration of IO critical for a country's success on the battlefield and influence in the international arena. At the strategic level, the military is one of the four instruments of state power: political, economic, military, and information. While the first three have been recognized as such for centuries, it is only recently that we have realized the importance of information among them. Information has integrative effects on the political, economic, and military aspects of power. It allows the state to coordinate and synchronize these powers when seeking the national interests. Information also becomes a necessity because it also describes the environment these powers will be used. Therefore, the lack of information may cause uncoordinated state powers to be used ineffectively.

The information also becomes an integrating instrument for the military power, allowing a coordinated, synchronized, and balanced use of resources in order to efficiently achieve the strategic objectives tasked by the President. IO is the embodiment of leveraging friendly information and information systems while denying the adversary the same benefits. The strategic level IO is directed by the President and planned in coordination with other agencies and organizations outside the Department of Defense.

This level can be seen as the top-level integration of political, economic, and military powers through information. The president determines the strategic objectives that will bring about the achievement of the national interests. The military leadership translates these strategic objectives into national military strategy. The goal of IO at this level is to engage adversary or potential adversary leadership to deter crisis and to end hostilities once they occur. While the strategic level efforts continue throughout all the phases of a conflict, operational level IO starts to become more relevant as hostilities mount to violent action. The operational level is concerned with employing IO in a theater of war or theater of operations to obtain an advantage over the enemy. IO at this level translates strategic objectives into tactical actions through conduct of strategies, campaigns, and operations. It can be very effective in the initial stages of a conflict, can help the tactics succeed smoothly, and can bring about a quicker and less damaging resolution to the hostilities. The tactical level deals with the details of prosecuting engagements in the changing environment of the battlefield, and IO becomes a force multiplier which improves the tactical effects tremendously. While relative superiority of numbers have always been a concern of commanders on the ground, IO at the tactical level can cause units to have disproportionate effects. Integration of different levels of IO causes the effects achieved at all levels to converge at the objective, so that the desired goals become easily attainable. Integration is the essence of resource optimization, effect maximization, and damage minimization.

B. PAST EXAMPLES OF IO

IO is not something new. Information has always been a part of military operations, but it has gained importance as people have relied more and more on it. For example the Golden Horde had one of the best communications system of its time, which helped Genghis Khan make timely and informed decisions to make them as effective as they were. WWII witnessed very good IO efforts especially in the deception schemes for Sicily and Normandy landings. Operation Mincemeat, "The man who never was," was a very ingenious and creative scheme to release a dead body with allied uniform on and with landing documents in the coast of Spain. This deception caused the Germans to perceive Greece as the probable allied landing site instead of planned Sicily. Another successful deception came with the Normandy landing which led Hitler to believe that

the intended landing would be in Pas de Calais instead of Normandy (Montagu 6). Both deceptions were very effective in causing the adversary to concentrate his forces away from the friendly landings. Furthermore, the Cold War was also a showcase of the dominance of information over attrition. At the strategic level, the US adopted an open policy which encouraged the free dissemination and debate of information while the USSR tried to suppress all informational channels. Even the military competition displayed a similar pattern. While the US and its allies developed flexible doctrines, strategies, and weapons (i.e., PGMs) which relied on importance of information, the Soviet Union adopted an overall strategy based on massing firepower and winning through attrition. The history proved the advantage provided by information superiority with the defeat of the Soviet regime (Arquilla and Ronfeldt 423). Below is the discussion of the Operation Desert Storm as a successful IO campaign example and the Operation Allied Force in Kosovo with its shortfalls in the IO effort:

1. IO in Operation Desert Storm

The Coalition forces used IO effectively in Operation Desert Storm. IO did not deter war, but the casualty figures definitely show how effective it was in reducing friendly damage. Before the war the goal of IO was to gain public support – support of the US public, the Arab nations and the international community as a whole. The US efforts were conducted through the UN and the media. The media extensively covered the critical events surrounding the hostilities and helped shape the public opinion. The public opinion about a possible war was positive right before the war, which shows the successful public affairs activities of the US government (Mueller 75). On the other hand, Iraqi propaganda and efforts to gain international support continued. Saddam Hussein's political strategy was aimed at influencing the decision-making of the Coalition national leadership. He tried to gain public support by defaming Kuwait's ruling family and portraying Iraq as the champion of anti-colonialism, social justice, Arab unity, the Palestinian cause, and Islam. Hussein's attempts to intimidate his neighbors were unsuccessful, and the Gulf States requested outside help and a coalition formed. The Coalition's effective use of information operations on all fronts to defend against Saddam's information strategy ensured that Iraq failed to ever seize the initiative (Joint Publication 3-13 I-20).

The Coalition integrated OPSEC and deception effectively to shape the beliefs of the adversary commander and to achieve surprise. The goal was to convince Iraqi leadership of the Coalition intent to conduct the main offensive using ground and amphibious attacks into central Kuwait by dismissing real indicators of the true intent to swing west of the Iraqi defenses in Kuwait and to make the main attack into Iraq itself. The OPSEC process showed that the Coalition force and logistic preparations for the ground offensive could not be hidden from Iraqi intelligence collection prior to initiation of the air offensive. The Coalition forces conducted the preparations in areas of Saudi Arabia logical for an attack into Kuwait. Then, the forces were postured for the main ground offensive into Iraq using the air offensive to blind most of the Iraqi intelligence collectors and to secretly move the force to the west where it would be. Deception would create false indicators and OPSEC would alter or hide real indicators with the purpose of leading Saddam Hussein to conclude that the Coalition would attack directly into Kuwait. Several deception measures were used: Broadcasting tank noises over loudspeakers and deploying dummy tanks and artillery pieces as well as simulated HQ radio traffic to fake the electronic signatures of old unit locations. OPSEC measures allowed selected Iraqi intelligence collectors to witness pieces of the final Coalition preparations for the real supporting attack into Kuwait and directed aggressive patrolling in this sector. The Marine force off the coast conducted both deception and OPSEC (Joint Publication 3-13 II-3). However, a lot of experts had speculated about the Coalition's possible courses of action in the media. The battle plan was inadvertently published in several well-known magazines, which represented a real threat to the whole OPSEC effort. Fortunately, the Iraqi intelligence did not realize this (Mueller 127).

PSYOP were also conducted successfully. The use of leaflets, radio and television broadcasts, and loudspeakers contributed to the surrender of 87,000 Iraqis. Table 4 and Table 5 display how effective these PSYOP efforts were.

The opening of the Coalition air campaign illustrates the use of IO at the tactical level. The capability of choice was EW supported by physical attack. The initial goal of the air campaign was to conduct SEAD so that the air strikes into Iraq could go smoother. The first phase before the war started involved "needling" missions close to the border in order to expose weaknesses in the Iraqi air defense system. The Coalition sent fighters

close to the border while RC-135s and other intelligence collectors observed the Iraqi response. These missions exposed one intercept center which did not communicate sideways to the adjacent centers. This was the weak point the Coalition air forces sought. 0300 hours on 17 January 1991 was the H-hour for the operation and the start of the coordinated series of attacks. Attack planes had their regular self-protection ED suite and were escorted by EF-111 and EA-6B jamming support planes. EA-6B Prowlers, F-4G Phantoms, F/A-18 Hornets, and A-7 Corsairs carried AGM-88 HARM anti-radar homing missiles for their assigned target areas. Also B-52s, each carrying 5 AGM-86 air-launched cruise missiles, were heading to their designated launch points from Barksdale Air Force Base. 38 Northrop BQM-74 decoy drones flying at medium altitude in fighter-type formations began heading towards defended areas. They were picked up by the Iraqi surveillance radars. When SAM sites and AAA engaged these drones, no fewer than 200 HARMs headed in their direction. The next act was conducted by 8 AH-64 helicopters attacking two early warning/ground controlled intercept radar stations with their Hellfire missiles initially and then with unguided missiles and 30 mm rockets. These radar sites belonged to the weak link mentioned above. Several Tomahawk missiles fired from the US warships conducted another supporting attack. These missiles released small spools of carbon fiber which caused their targets (selected electricity switching stations) to short circuit. The air operations centers in that area were affected by the blackout and ceased to function until their generators came online. The first night was a success with 671 manned aircraft sorties flown, only one aircraft lost to another plane, and most of the Iraqi air defense suppressed (Price 202-207).

These were part of the IO campaign in the Desert Storm and contributed to the ultimate victory of the Coalition forces.

	Leaflets	Radio	Loudspeakers
% Exposed to PSYOP	98	58	34
% Believed PSYOP	88	46	18
% Influenced to Act	70	34	16

Table 4 PSYOP Impact on Surrenders (From Psychological Operations during Desert Shield/Storm: A Post-operational Analysis 1)

Gulf War Leaflet Drops (millions)					
Themes	**Balloon**	**MC-130**	**F-16**	**B-52**	**Total**
Surrender	0.0054	11.5	0.81	0	12.364
Inevitability	0	4.3	2.3	0	6.6
Abandon Equip./Flee	0	1.3	0.585	0	1.885
Saddam's Fault	0.09	1.8	0.535	2	4.425
Other	0.186	0	3.3	0	3.486
Total	0.33	18.9	7.53	2	28.76
Note: It is estimated that 98% of 300K Iraqis targeted were affected by leaflets					

Table 5 Gulf War Leaflet Drops (From Psychological Operations during Desert Shield/Storm: A Post-operational Analysis 1)

2. IO in Kosovo: Operation Allied Force

Another example could be the use or misuse of IO in the planning for the Kosovo campaign. This massive air campaign was carried out by a coalition of United States and NATO air forces against the former Yugoslavia over its policies of genocide in the province of Kosovo. The coalition inflicted massive destruction on Serbia's economic infrastructure with over 34,000 combat sorties in a 78-day period of bombing. However, NATO's operation created greater regional instability and the potential for future conflicts because no concerted peacetime IO campaign was implemented to deter conflict with Serbia. IW was successfully executed throughout the conflict in order to bring the conflict to a peaceful conclusion. IW tends to rely heavily on physical destruction supported by other IO capabilities and related activities. Since no concerted peacetime IO campaign against Serbia was executed, inflicting severe damage due to physical destruction could not be avoided. These damages ultimately made a post-conflict period much more difficult to manage both politically and economically (Joint Command, Control and Information Warfare School 100).

IO is a long-term strategy that must be put into motion during peacetime, but an overall information strategy was never attempted against Yugoslavia despite almost

seven years of warning. While the United States was struggling towards a national IO strategy and was suffering from lack of political direction at the time, it was not ready to coordinate a strategy with NATO on top of its struggles (Hubbard 57). As a result, there was no clear link between military and political strategy of NATO. This caused impatience with the diplomatic process and inhibited the execution of an IO strategy. Serious blunders were made at the operational level which precluded the long-range planning of an IO campaign. The ground forces were ruled out and, therefore, the alternatives for OPSEC and deception were reduced even before the campaign began. Contingency planning lacked in addressing the public relations aspects of military failures, i.e. the Chinese embassy bombing. NATO PA personnel also never connected the Danube bridges' destruction to protecting the Hungarian minority in Vojvodina. The resulting confusion following those incidents greatly damaged NATO's credibility. The advent of PGMs and effects-based targeting has transformed physical destruction from an attrition method to be an information weapon. It demonstrates the precision, lethality, and superiority of the friendly weapons technology while limiting collateral damage and physical destruction, thus, provides less of a ground for hostile propaganda. On the other hand, the international media will tend to amplify the effects of an accident when the occasional accident occurs and a nonmilitary target is hit by a country that has the technological means to minimize civilian casualties. When physical destruction takes place, it is critical that the public affairs and PSYOP messages describing the use of physical destruction be absolutely accurate. NATO also lost credibility when its press releases about destroyed Yugoslav weapons and vehicles did not match the "ground truth." Given that the National Army force in Kosovo was the target of the PA and PSYOP efforts, any loss of credibility with the target audience ultimately harmed these operations. The NATO Secretary General did not appear in the United States media in the beginning of the campaign, which also caused a perception of lack of unity in the coalition. These and other mistakes prevented the conduct of a viable IO campaign against Milosevic and his forces (Joint Command, Control and Information Warfare School 102). NATO achieved only the last two of the following objectives it had established in relation to the conflict with Yugoslavia:

- A verifiable stop to all military action and the immediate end of violence and repression;
- The withdrawal from Kosovo of the military, police and paramilitary forces;
- The stationing in Kosovo of an international military presence;
- The unconditional and safe return of all refugees and displaced persons and unhindered access to them by humanitarian aid organizations; and
- The establishment of a political framework agreement for Kosovo on the basis of the Rambouillet Accords, in conformance with international law and the UN Charter (Hubbard 59).

C. CONCLUSIONS

The above examples of IO application clarify several of the points discussed in the previous chapters of this thesis:

Strategic Level IO is very important in achieving the national objectives and winning/losing the conflict. As seen in the first example, achieving the initial objective of gaining public and international support paved the way to the ultimate victory. Even his Arab neighbors isolated Saddam. Also the formation of a coalition created an ownership to the cause by the Arab nations and the rest of the world. On the other hand, in Kosovo lack of a strategic level peacetime IO limited the achievable goals.

Peacetime IO needs to be planned and coordinated among agencies and coalitions, so that a coherent and successful IO can be conducted. The importance of this point is clearly visible in both cases.

Actions at a certain level may have effects at the higher levels. Failure of the tactical SEAD could destroy the deception scheme in Desert Storm while tactical bombing mistakes exacerbated by inefficient PA had strategic effects in Kosovo.

IO efforts continue at all levels simultaneously. Deception and OPSEC planning in Desert Storm was in the operational level while tactical air commanders were planning their SEAD mission. Meanwhile the president was probably trying to keep together the coalition which supported all these activities.

IO supporting capabilities must also be included in the integrated IO campaign planning without degrading their credibility. The PA personnel of Operation Allied Force had the impression that they could be used as a part of media manipulation and did not

attend IO meetings. Exclusion of PA personnel is not efficient because they will have a harder time doing their job if something goes wrong (Pounder 65).

Integration of IO at all levels will produce better results. Iraq case is obviously an example of that and is much more successful than the Kosovo case.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY AND CONCLUSIONS

A. SYNOPSIS

This thesis has explored the idea whether a balanced systematic approach is a better way to integrate IO at different levels of war compared to uncoordinated efforts at each level. In order to clarify this idea, it first provided background information on IO. After pointing out the increasing interest in IO, this thesis provided a few key definitions like information and information operations. A more detailed analysis of IO including OODA loop and information superiority concept followed. Waltz's basic engagement model was presented in order to better understand the information superiority concept. This model was illustrative of avenues of attack in IO. Following the advantages gained through information superiority was the explanation of offensive and defensive IO. The next topic was the introduction to the capability based approach used in the analysis of each level of warfare in this thesis. The final part of the background was the extended model of IW which included the society, media, and authority as a part of the target set besides the military.

The next three chapters followed a similar pattern in analyzing the IO at the strategic, operational, and tactical levels of warfare respectively. First a brief discussion of each level was provided. Characteristics of IO at that level followed the general discussion. Specific desired effects were sampled for each level. These effects formed the bond between that level and different IO capabilities. The discussion of which capabilities would be available for the desired effects followed a brief explanation of how those capabilities fit into that level of warfare. Sample systems were provided for each capability when appropriate.

Chapter V focused on past examples of IO. Operation Desert Storm was the example of a well-integrated IO effort while Operation Allied Force exemplified a lack of coordination in the different levels of IO. While the first one achieved its objectives, the second one was a disappointment and caused more instability in the region.

B. SUMMARY OF CONCLUSIONS

First there was only the infantry, and warfare was simple: Have more or stronger soldiers than your adversary's and you will gain relative superiority, which leads to victory. Even then IO was possible in some sort of deception, PSYOP, and OPSEC. Such a prehistoric IO would help you optimize your power while minimizing the adversary's through surprise, reduction of will to fight, etc. Now warfare is more complicated: While combined arms – integration of different branches in one service – would suffice in the near past, nowadays, joint and even interagency operations capability is deemed necessary for success. This illustrates a trend in the military art in the form of integration of different services and agencies, so that their multiple capabilities can be coordinated to achieve the national objectives. IO takes this integration one step further by coordinating and synchronizing them in the informational dimension that is the link to understanding the environment they have to operate in. Information and information systems day by day become more relevant and critical parts of that environment. There are opportunities to be exploited and inherent vulnerabilities to be protected. IO is an evolutionary concept which opens our eyes to this fourth dimension and when successfully applied, brings about a better integration and more efficiency to the capabilities of friendly forces. Here are several conclusions from this thesis on IO:

A balanced systematic approach to IO through its integration at all three levels of warfare will produce much better results than the uncoordinated cases.

IO has an integrative effect on the instruments of national power and the military capabilities at different levels of warfare.

Strategic level IO tries to prevent IW, while required operational level IO works to make conflict less damaging and end quicker by relating strategic objectives to tactical actions. Tactical level IO is a great force multiplier in winning the tactical battles.

IO efforts can continue at all levels simultaneously. Their integration will produce better results and improve the efficiency of the IO at the other levels.

IO efforts at one level can also have impacts on the other levels.

C. AREAS FOR FURTHER RESEARCH

IO is still in its baby steps and there are a lot of issues that require deeper analysis. Here are a few of those areas:

- If integration is the key to success, would it be a better way to organize according to capabilities rather than according to the traditional services?
- How can we best achieve the integration of IO capabilities?
- Different services bring different capabilities. What would be the best way to implement joint level integration and reduce the time lag?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

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

Alger, John I. "Information Assurance Evolves From Definitional Debate." *Information Assurance Technology Newsletter* Jul 97: 2-4.

Arquilla, John and David Ronfeldt, ed. *In Athena's Camp: Preparing for Conflict in the Information Age*. Washington, DC: RAND, 1997.

Biddle, Stephen. "Land Warfare: Theory and Practice." *An Introduction to Strategic Studies*. New York: Oxford University Press, 2002.

Boot, Max. "The New American Way of War." *Foreign Affairs* July/August 2003: 41-58.

"Critical Foundations: Protecting America's Infrastructures." *The Report of the President's Commission on Critical Infrastructure Protection*. October 1997.

FM 3-0, Operations. Washington, DC: Department of the Army, 14 June 2001.

Hall, Wayne M. *Stray Voltage: War in the Information Age*. Annapolis, MD: Naval Institute Press, 2003.

Hammond, Grant T. "The Essential Boyd." *War, Chaos, and Business*. 14 Aug. 2003 <http://www.belisarius.com/modern_business_strategy/hammond/essential_boyd.htm>.

Harley, Jeff. "Space Control and Information Operations." *Space Journal*. 15 Aug. 2003 <https://www.armyspace.army.mil/SpaceJournal/Article.asp?AID=19>.

Hubbard, Zachary P. "Information Warfare in Kosovo." *Journal of Electronic Defense* Nov 1999: 57-59.

"JFSC JCIWS IW Divison-IO Timeline." *The Information Warfare Site*. 14 Aug. 2003 <http://www.iwar.org.uk/iwar/resources/jfsc/io-timeline.htm>.

Joint Command, Control and Information Warfare School. *Information Operations: The Hard Reality of Soft Power*. Norfolk, Va: National Defense University Joint Forces Staff College, 2002.

Joint Publication 1-02, DOD Dictionary of Military and Associated Terms. Washington, DC: Joint Staff, amended 5 June 2003.

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

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

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

Joint Publication 3-53, Doctrine for Joint Psychological Operations. Washington, DC: Joint Staff, 10 July 1996.

Joint Publication 3-54, Joint Doctrine for Operations Security. Washington, DC: Joint Staff, 24 January 1997.

Joint Publication 3-57, Joint Doctrine for Civil-Military Operations. Washington, DC: Joint Staff, 8 February 2001.

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

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

McNeive, James F. "Information operations at the tactical level." *Marine Corps Gazette* Jun 2003: 52-53.

Montagu, Ewen. *The Man Who Never Was: World War II's Boldest Counterintelligence Operation.* Annapolis: Bluejacket Books, 2001.

Mueller, John. *Policy and Opinion in the Gulf War.* Chicago: The University of Chicago Press, 1994.

Pounder, Gary. "Opportunity Lost: Public Affairs, Information Operations, and the Air War against Serbia." *Aerospace Power Journal* Summer 2000: 56-77.

Price, Alfred. *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present.* London: Greenhill Books, 2001.

Psychological Operations during Desert Shield/Storm: A Post-operational Analysis. MacDill Air Force Base, Florida: USSOCOM, 5 November 1993.

Sun Tzu. *The Art of War*. Trans. Lionel Giles. *The Internet Classics Archive.* Massachusetts Institute of Technology. < http://classics.mit.edu/Tzu/artwar.html>.

"Three Levels of War." *Essays on Air and Space Power.* Ed. Air University. Maxwell Air Force Base, Alabama: Air University Press, 1997. 13-21.

Waltz, Edward. *Information Warfare: Principles and Operations.* Boston: Artech House, 1998.

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY

Campaign: A series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space.

Defense Information Infrastructure: The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The Defense Information Infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information.

Global Information Infrastructure: The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure.

Information Operations (IO): Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Warfare (IW): Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

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.

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.

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.

National Information Infrastructure: The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure.

Operation: 1. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. 2. The process of carrying on combat, including movement, supply, attack, defense, and maneuvers needed to gain the objectives of any battle or campaign.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Prof. Daniel Boger
   Naval Postgraduate School
   Monterey, California

4. Steve Iatrou
   Naval Postgraduate School
   Monterey, California

5. Kara Kuvvetleri Komutanligi
   Kutuphane
   Bakanliklar, Ankara, TURKEY

6. Kara Harp Okulu Komutanligi
   Kutuphane
   Bakanliklar, Ankara, TURKEY

7. Deniz Harp Okulu Komutanligi
   Kutuphane
   Tuzla, Istanbul, TURKEY

8. Hava Harp Okulu Komutanligi
   Kutuphane
   Tuzla, Istanbul, TURKEY

9. Orta Dogu Teknik Universitesi
   Kutuphane
   Inönü Bulvari, Ankara, TURKEY