ACSC/DEC/124/96-04

INFORMATION WARFARE: PLANNING THE CAMPAIGN

A Research Paper

Presented To

The Directorate of Research

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Lt Col Fredrick Okello
Maj Richard Ayres
Maj Patrice Bullock
Maj Brahim Erhili
Maj Bruce Harding
Maj Allan Perdigao

April 1996

Disclaimer

The views expressed in this academic research paper are those of the authors and do not reflect the official policy or position of the US Government or the Department of Defense.

Contents

Page

Illustrations

Page

Tables

Page

Preface

We selected this research project to refine our understanding of how information warfare relates to the selection of centers of gravity. Our initial expectation was that a method for devising an information warfare campaign already existed and that we would be investigating a single aspect of it. We quickly discovered this is not the case. As a result, our desire to help planners identify information warfare centers of gravity led us to build a step-by-step approach to planning a whole campaign. We hope this product will be a useful tool for the planner at any level who is tasked to create an information warfare campaign, as well as for anyone wishing to understand the process for planning such a campaign.

We also want to express our sincere thanks to Dick Ayres. Through lighting storms, power outages, and corrupted files, he managed to keep his sanity.

Abstract

Information warfare is a nebulous concept, but widely cited as a keystone in any future campaign. Even though information warfare has been used for centuries, current doctrine, policies, and guidance provide little help for the warrior to understand first, what information warfare is, and secondly, how to do it.

"Information Warfare: Planning The Campaign" provides a logical approach for the information warrior to employ in planning for this aspect of warfare. This paper addresses the:

- Current state of information warfare policy and doctrine,
- Modeling of a system to identify its critical nodes and links,
- Modeling of a Joint Forces Air Component Commander (JFACC) to serve as an example,
- Examples of current and potential offensive and defensive information warfare tools used in information encounters, and finally,
- A step-by-step approach to information warfare campaign planning.

Analysis of information and its flow is a daunting undertaking in all but the most simple of organizations. To remedy this, one can view the organization as a system and employ a model which will help illustrate information flows. It is reasonable to employ the same model for this purpose as is used by system engineers who create information systems. This paper describes such a model, the Operational Architectures Model, which employs the *I*ntegrated Computer Aided Manufacturing (ICAM) *DEF*inition Methods or IDEF for short, to identify the flow of information in a system. Internal to the Operational Architectures Model are five modeling perspectives: functional, physical,

static, informational, and dynamic. The functional perspective identifies what functions a system must accomplish to achieve its overall purpose. The physical perspective establishes what assets the system uses to accomplish its purpose. Combining these assets with the functions they support produces the static perspective, a view of the system at rest. The informational perspective assesses the structure of the information needed to support the functions of a system. Finally, the dynamic perspective models the performance of the system over time. Going beyond a theoretical discussion of this complex model, the paper then provides a concrete example by using the model to analyze a Joint Force Air Component Commander.

As stated earlier, information warfare has been around for centuries. To help clarify the concept of information warfare in today's environment, the paper describes current and potential information warfare tools. Understanding the tools and where they can be effectively employed provides a strong foundation in building an understanding of information warfare.

The final chapter brings the discussion to closure by providing a 4-step method for information warriors to use in planning an information warfare campaign. It employs the Operational Architectures Model to help the planner identify centers of gravity and match information warfare tools to those centers of gravity. The end product is a campaign which employs information warfare to protect or attack informational centers of gravity.

Chapter 1

Introduction

Warfare is an art, not a science. Yet the newest frontier of warfare, information, blurs the distinction between the two and draws them together in a new way. Proponents of information warfare argue its virtues and decisive nature in a way remarkably similar to the early (and some contemporary) proponents of airpower's capabilities. This chapter surveys the current status of thinking on information warfare, especially within the Department of Defense.

The roots of information warfare are old and deep. Warriors and strategists have long recognized the role of knowledge in warfare. Indeed, the age-old warfare principles of surprise and security embody the creation and exploitation of an information differential. Sun Tzu believed this to be a critical condition for defeating one's enemy and described the increase in peril as information dominance decreases:

> Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.[1]

History is replete with examples of warriors who successfully exploited an information differential to defeat their foes. For example, Hannibal used signal mirrors during the Second Punic War to keep track of Roman movements. As a result, he continually enjoyed the benefit of decisive tactical surprise.[2] A more recent example is

the Allies' exploitation of ULTRA to decode intercepted high level German communications during World War II.

Though the importance of increasing one's own knowledge while limiting the enemy's has long been realized, it has historically been ancillary to other operations. Something has changed which allows us to consider information warfare in a new, more comprehensive light. That something is the proliferation, increasing sophistication, and growing connectivity of modern information systems. This has created a situation where, for the first time, an information realm exists within which we can conduct widespread military operations.[3] What the information warrior is attempting to do may be old, but the technologies which he or she uses to do it are new, as is the battlespace in which the operations are conducted.

Within this new battlespace, information warfare seeks to obtain information dominance. Its scope includes both offensive and defensive operations. The National Defense University has devised a working definitions for information warfare:

> Information-based Warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based Warfare is both offensive and defensive in nature—ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets.
>
> While ultimately military in nature, Information-based Warfare is also waged in political, economic, and social arenas and is applicable over the entire national security continuum from peace to war and from 'tooth to tail.' Finally, Information-based Warfare focuses on the command and control needs of the commander by employing state-of-the-art information technology such as synthetic environments to dominate the battlefield.[4]

The new technologies and battlespace offer more than just effective large-scale pursuit of old information missions. There are two aspects to information warfare into

which both offensive and defensive operations fit. The first is indirect, wherein one affects an enemy's information via his perceptual and analytical processes.[5] This can mean depriving the enemy of the ability to observe, as when one employs jammers or destructive means against radars. Alternatively, one can feed false information into the enemy's information collectors, causing him to believe something false or disbelieve something true. An excellent example of this is the use of decoys or employment of camouflage. In either case, the information warrior relies on the adversary's perceptual and analytical mechanisms to manipulate his information.

There is a second aspect to information warfare. The potential now exists to directly manipulate an enemy's information, bypassing his perceptive, analytical, or decision processes.[6] "If information warfare means something new, it is the use of information as a substitute for traditional ways of fighting, rather than as an adjunct to them."[7] Direct information warfare incorporates some of the more exotic techniques such as computer viruses, logic bombs, or hacker attacks. Some believe these techniques are visionary, yet the news media have reported possible instances of their use. For example, US News and World Report claims to have obtained information that US intelligence agents successfully infected Iraq's air defense computer network with a virus which caused information windows to go blank.[8]

Views differ on what, if anything, this all means. Some greatly downplay the significance of information warfare. For example, Martin C. Libicki of the National Defense University argues that defenses against direct attack can be installed on important computer systems. These defenses will improve with experience gained in protecting systems from criminal attacks and will likely prove effective against hostile

attacks as well.[9] What is more, in his view, information warfare does not form a separate technique for warfighting. Lack of clarity in definitions of terms has allowed an incoherent conglomeration of forms for attacking information to be subsumed under the single term of information warfare, each form claiming to be the "real" information warfare. He rejects the idea that a information has become an independent realm for the waging of war.[10]

On the other hand, his colleague, Paul A. Strassmann, visiting professor of information warfare, believes that not only is direct information warfare a significant threat, but said the United States has already been subjected to it.[11] Winn Schwartau heartily agrees. In his book, *Information Warfare*, he describes a nightmare world of information warfare on three levels—personal, corporate, and global—which he believes already exists.[12] The development of a global system of computers has created something new, an information battlefield which he calls cyberspace.[13] Futurists Alvin and Heidi Toffler concur that a new form of warfare has emerged. In *War and Anti-War*, they describe the emergence of "knowledge warriors" who are formulating "knowledge strategy" which will be the key to victory in future wars.[14] According to John Arquilla of the Naval Postgraduate School,

> . . . information dominance has always 'mattered,' but . . . a variety of factors have now converged to enable it to fulfill its potential to achieve overarching effects in the realm of conflict.[15]
>
> Today, . . . the opportunity exists to transform knowledge into capability via information dominance. Indeed, the fundamental nature of war-fighting will undergo radical changes because of the effects, properly wielded, of information dominance, which will succeed, subsume and transform many of the effects derived from its principal predecessors, sea and air power.[16]

Though some scholars disagree on whether information warfare inhabits a discrete realm and whether it represents a new form of warfare, the United States Department of Defense has clearly concluded both propositions are true. Information warfare has generated broad interest, with the result that, "Information-war studies are proliferating within the American armed forces almost as quickly as the networks that carry them from desktop to desktop."[17] One primary stimulus for this interest lies in the success of the Persian Gulf War, often referred to now as the first information war.

At the joint level, organizations such as the National Defense University's (NDU) School of Information Warfare and Strategy have been created to focus research on the subject. Other examples of joint study centers for information warfare are found in the Defense Information Systems Agency and the Advanced Research Projects Agency.[18] Each of the services has also adopted organizational structures to examine integrating information war into its operations, such as the Air Force Information Warfare Center. Numerous symposia and articles in military journals attest to the interest this form of warfare now enjoys within the Department of Defense.

Despite this interest, information warfare remains in a nascent state, lacking the body of definitive policy and doctrine drawn from experience which characterizes more mature forms of warfare. The current state of policy flux is described by Martin Libicki:

> Since March 1993, Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30 (MOP 30) has set forth definitions and relationships that have guided the joint community in its thinking about the related concepts of information warfare and command and control warfare. As these seminal ideas have evolved, their definitions and relationships have changed as well. MOP 30 is under revision, and both higher level policy documents for the Department of Defense and doctrinal publications of the Joint Staff and Services are either in draft form or under revision.[19]

Legal guidance also remains unclear. As Daniel Kuehl, professor at the School of Information Warfare and Strategy at NDU asks, "What is an act of war in the information age? Nowhere is that defined. Has the technology outpaced existing laws? Of course."[20] In light of this, Air Force Chief of Staff General Ronald Fogleman noted the difficulties this causes in developing new doctrine. "Because exploiting [information systems] will readily cross international borders, we must be cognizant of what the law allows and will not allow. We must have good legal advice as we get into this."[21]

With policy and doctrine still being born, combatant commanders face a difficult problem. Absent fully developed policy and doctrine, commanders in chief (CINCs) of the combatant commands were largely waiting to employ information warfare in their exercises. Now, however, they have been instructed to integrate information warfare into their training and exercise programs even without definitive guidance.

It is the intent of this paper to help not only CINCs' planners, but also planners of information warfare campaigns at any level of warfare and in virtually every context to employ information warfare even in the absence of mature doctrine. This paper offers an analytical model planners can employ to identify key informational nodes and links, allowing them to assess both friendly and enemy vulnerabilities. For clarity, it supplies a concrete example by examining a Joint Force Air Component Commander's information system through the eyes of this model. For practical purposes, it describes the information warrior's "toolbag" which, though certainly not all-inclusive, should provide a reasonable starting point for planning the conduct of information warfare. Finally, it describes a step-by-step process for combining the model and the toolbag with objectives and assessment, resulting in an information warfare campaign. Though this cannot make

up for the fluid and rudimentary nature of information warfare policy and doctrine, it can perhaps bridge the gap and assist in the exercise of information warfare until authoritative guidance has been fully elaborated.

Notes

[1] Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith, Oxford University Press, Oxford, 1963, 84.

[2] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review*, Summer 1994, 25.

[3] Department of the Air Force, "Cornerstones of Information Warfare," 1995, 8-9.

[4] Working definition recognized by the Information Resources Management College of the National Defense University as of 11/16/93, Internet: http://vislab-www.nps.navy.mil/~sdjames/IW/Definition.html.

[5] Cornerstones, 4.

[6] Cornerstones, 4.

[7] "The Ties That Bind," *The Economist*, June 10, 1995, 18.

[8] "The Gulf War Flu," *US News & World Report*, January 20 1992, 50.

[9] Martin C. Libicki, What Is Information Warfare (Draft), National Defense University, 21 July 1995, 22.

[10] Libicki, 34.

[11] "Information Under Siege," *Computerworld*, June 5 1995, 55.

[12] Winn Schwartau, *Information Warfare*, Thunder's Mouth Press, NY, 1994, 17-20.

[13] Schwartau, 49.

[14] Alvin and Heidi Toffler, *War and Anti-War*, Warner Books Inc., NY, 1993, 166.

[15] John Arquilla, "The Strategic Implications of Information Dominance" *Strategic Review*, Summer 1994, 27.

[16] John Arquilla, 29.

[17] "The Ties That Bind," *The Economist*, 10 June 1995, D18.

[18] Daniel E. Magsig, Information Warfare In The Information Age, Internet address: www.seas.gwu.edu/infowar.html.

[19] Martin C. Libicki, What Is Information Warfare, May 1995, Internet address: http://www.ndu.edu/ndu/inss/strforum/forum28.html.

[20] Daniel T. Kuehl, quoted by Gary H. Anthes in "New Laws Sought For Info Warfare," *Computerworld*, June 5 1995, v29, n23, 55.

[21] Gen Fogleman, quoted by Anthes, Ibid.

Chapter 2

Information Warfare Modeling

> *The scene is 1988. An energetic, forward-thinking young man wants to enter the new computer age and thus visits a local computer store. The store salesman approaches the young man and asks how he may be of assistance. The young man replies "I need a computer—probably a 386; what model do you recommend?" The salesman returns with a question—What do you want the computer to do for you? The young man, puzzled if not deflated, replies, "I just need a computer."*

In many ways the Department of Defense (DOD) is in a similar situation with regard to information warfare. It is certain it needs to use information warfare, but it is not entirely clear on how or why. As pointed out in the previous chapter, the DOD has not yet been able to fully determine what it wants to get from information warfare, or how it wants to get it, in part because of the lack of agreement on what it is, and in part because a wealth of historical experience does not yet exist. Nevertheless, the DOD is trying to proceed with integrating information warfare into its operations with as much speed as possible.

Ask a majority of military officers to define information warfare. The answer will commonly be phrased in the popular public vernacular of "hackers," "viruses," or as "putting viruses in the enemies computer systems to achieve our military objectives." A further question beyond the first will almost invariably yield a shoulder-shrug. Clearly, given the emphasis and resources going towards it, the DOD is on the information

warfare course full throttle. However, much of the military lacks the commonly understood intellectual framework and doctrine required to plan, conduct, and defend against information warfare. Thus, for many of those required to actually plan for the conduct of information warfare, it is a case of all throttle and little or no vector.

One of the major elements missing in the information warfare framework is a method to analyze oneself or one's opponent to identify critical nodes which must be defended or are vulnerable to attack. In view of this, the purpose of this chapter is to introduce a systems analysis model known as the Operational Architectures Model to aid the military in planning, conducting, and defending against information warfare. For clarity, the model will then be used in the following chapter to analyze an operational element of the US military with which many people have at least passing familiarity, a Joint Force Air Component Commander as was seen in Desert Storm.

Review of Campaign Planning and the Systems Approach

Clausewitz stated "the first task, then, in planning for war, is to identify the enemy's center of gravity (COG), and if possible, then trace them back to a single one."[1] The best method to analyze and identify an enemy's and one's own COGs is to employ a systems analysis approach. This approach is the common method used by virtually all military campaign planners. Though specific analytical models differ, the utility of viewing oneself and one's enemy as a system, thus identifying critical nodes and linkages, is universally taught in schools of professional military education. We must begin our discussion by defining what a system is, as well as some other related terms.

In *The Systems Approach—A Primer*, a *system* is defined as a "collection of interrelated parts which is unified by design to obtain one or more objectives" or an "organized or complex whole; connotes plan, method, order, and arrangement."[2] *Systems analysis* is then, "an inquiry to aid the decision maker in choosing a course of action by systematically investigating one's objectives, comparing quantitatively where possible, the cost effectiveness and risks associated with alternative policies or strategies for achieving them, and formulating additional alternatives if those are found wanting."[3]

For the military planner, centers of gravity are identified and courses of action are developed by conducting a systems analysis on himself and his opponent. The mechanism by which a systems analysis is conducted is the employment of models to represent the behavior of systems. A *model* is simply a representation of a system, be it mathematical, physical, or descriptive. The *fidelity* of a model is the degree to which a model realistically represents the system it is modeling; it is not necessarily synonymous with a model's level of detail or complexity. Before campaign planners begin modeling a system, five questions require review:

1. the particular problem at hand,
2. the purpose of the model,
3. the model's objectives,
4. the model's boundaries and level of detail, and
5. the particular viewpoint or perspective of the modeler.

Considerations used in devising a model are illustrated in Figure 1.

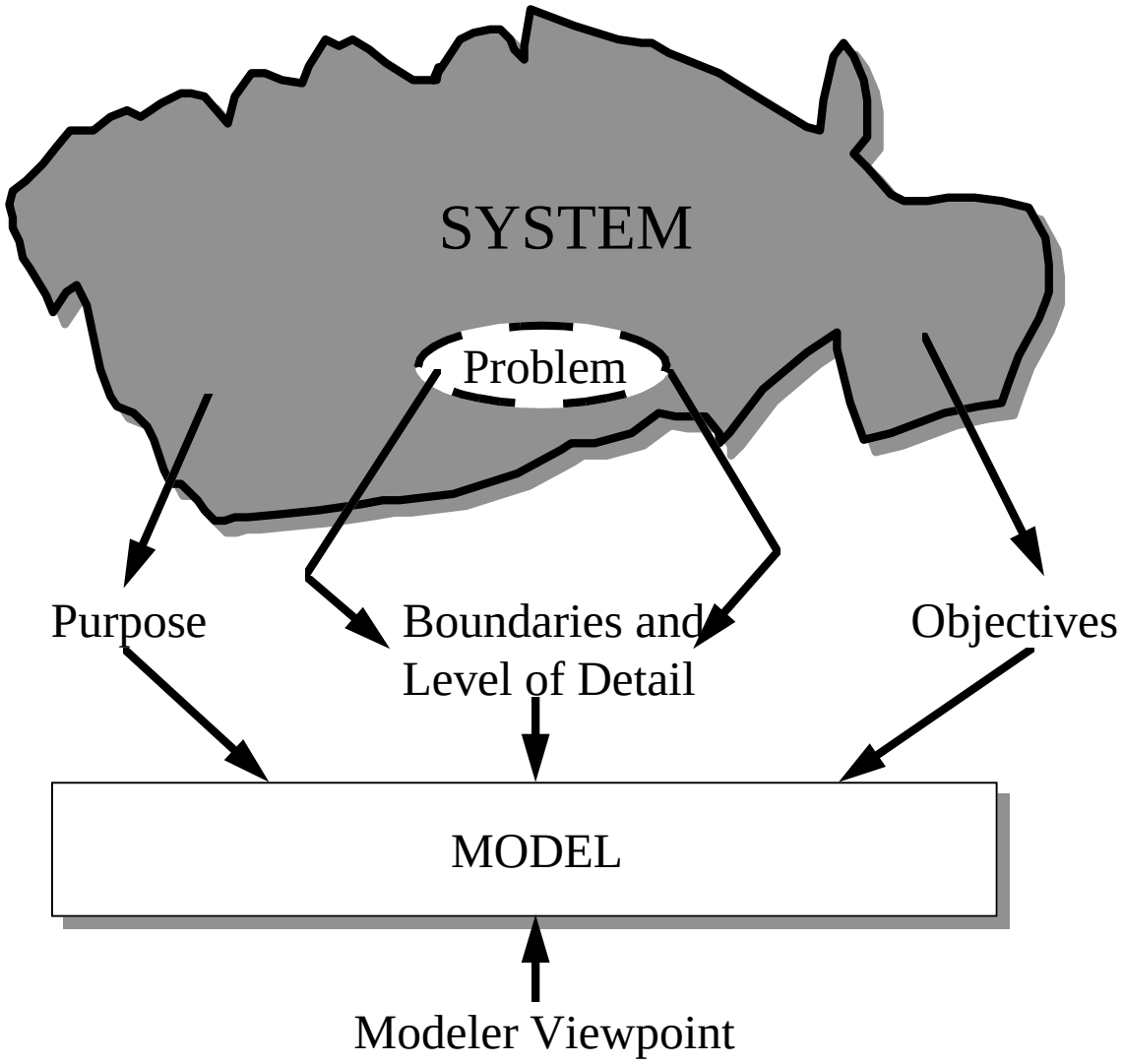

Figure 1. Approach to Model Building[4]

An example of a system model is Col John Warden's "Five Rings"—where any system from a human body to a solar system can be represented by five components (rings) organized concentrically in order of importance from the center: leadership, organic essentials, infrastructure, population, and fighting mechanism.[5] This is an example of a medium fidelity model which is simple, if not elegant. However, models such as Warden's do not make the concept of information warfare obvious to the planner. Useful for analysis of an enemy's physical or morale structure, this type of model devotes

little attention to the informational linkages between and within the rings. Only by continued elaboration of the analysis to lower and lower levels do such linkages begin to emerge. As a result, the very crux of the information warrior's interest, informational nodes and linkages, may remain obscure.

For those attempting to plan an information warfare campaign, a different model is needed—one which explicitly depicts the flow of information. Fortunately, such a model is readily available in the form of the Operational Architectures Model, a modeling framework common to commercial and government system engineers as well as computer hardware and software designers. It is intended to fully model informational systems from the perspective of those who must design and integrate them. This, then, also makes it ideal for the purposes of those who wish to understand extant systems.

Concept of Operational Architectures

A system can be described and modeled by architectures. Although there are many definitions of the term *architecture*, for the purposes of this discussion it refers to a single-dimensional view of a system. This view, when combined with other single-dimensional views of the system in a building block approach, then provides one with the system's *architectures* (plural). For example, if one wished to understand a human being as a system, one could begin with evaluating the physical structure, i.e., the body, a single-dimensional view. For fuller understanding, one would also have to assess the mental processes—the thoughts and emotions—another single-dimensional view. These two views, when combined, provide a more comprehensive understanding than either of

them did by themselves. The final product of this is called the system's operational architectures.

The key to making such an approach work lies in the careful selecting each of the single dimensions along which one will view the system and the correctly combining them into an overall view of the system (its architectures) which identifies the relationships between each component architecture. For information warfare planning, the term *operational architectures* refers to models which describe the behavior of a system by analyzing five architecture elements (i.e., five single-dimensional views): the functional, physical, operational (static), data/informational, and the operational (dynamic) architectures. Underlying these architectures is the operational concept of the system—it purpose. This model is depicted in Figure 2.

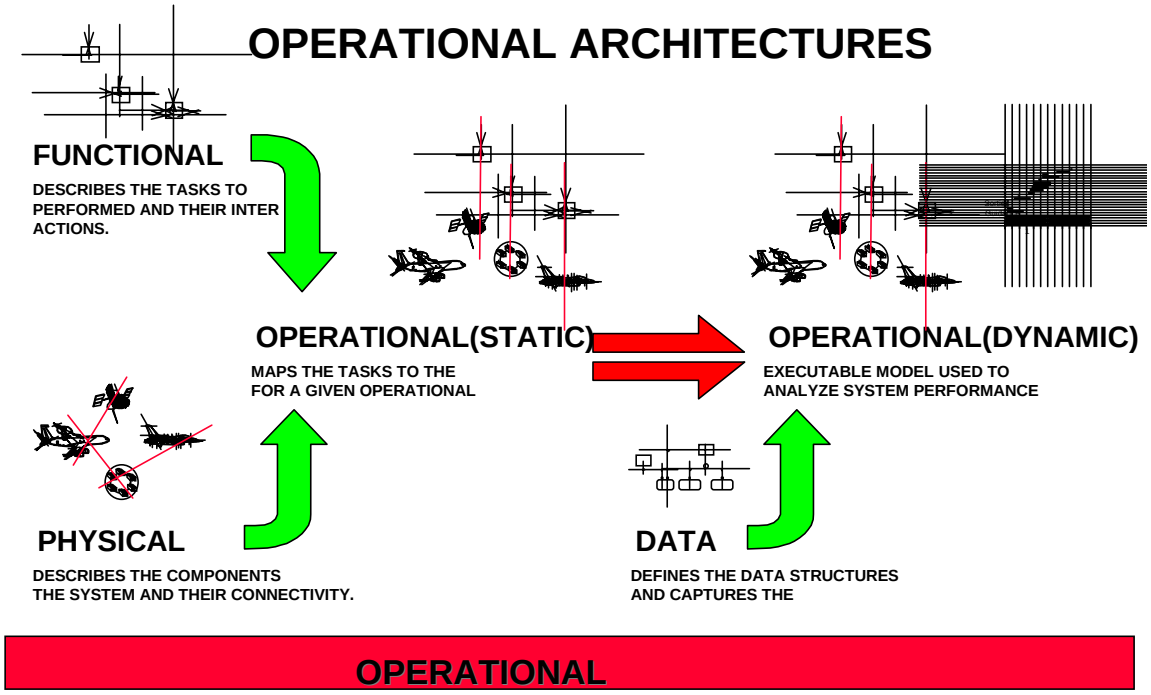

Figure 2. Operational Architectures Model

The specific family of modeling methods used to apply the Operational Architectures Model to informational systems is known as *I*ntegrated Computer Aided Manufacturing (ICAM) *DEF*inition Method, or IDEF.

*I*ntegrated Computer Aided Manufacturing (ICAM) *DEF*inition Method (IDEF)

The concept of operational architectures and IDEF is not new. The IDEF method was actually developed in 1981 by the once classified US Air Force Program for ICAM to "increase the manufacturing productivity through the systematic application of computer technology."[6] As public, industry, and government awareness of computer applications and technology improvements progressed, use of the IDEF method expanded. For

example, in the 1980s, the DOD applied the method in its Strategic Defense Initiative program to develop and integrate the complicated architecture, or "system of systems," used to execute time-constrained operations of multi-layered weapon systems, communication platforms and computers for ballistic missile defense. By 1990, the DOD embraced IDEF methods as the standard for creating all its information systems. In applying the IDEF method, the DOD explicitly recognized its relationship to offensive and defensive information warfare, stating, "The DOD has long recognized the opportunity for significant technological, economic, and strategic benefits attainable through the effective capture, control, and management of information and knowledge resources.…Like manpower, materials, and machines, information and knowledge assets are recognized as vital resources that can be leveraged to achieve competitive advantage."[7]

IDEF is organized into three sets of modeling methods, each modeling different aspects (or perspectives) of a system. The first, $IDEF_0$, models the functional and physical architectures, resulting in the operational (static) architecture of the system. $IDEF_1$ is used to model the data and information architecture. Finally, $IDEF_2$ models the operational (dynamic) architecture of the system. Each of these architectures and the associated IDEF methods are discussed in more detail below.

If military planners are to attack or defend information systems, they must have the proper framework to understand the systems and recognize the effects of attacks against specific elements of them. The Operational Architectures Model, utilizing IDEF methods, provides that framework.

Explanation of Operational Architectures Elements Using IDEF

As discussed earlier, operational architectures are models which describe the behavior of a system using five single-dimensional views, or architectures. Another way to view each individual architecture is as layers of a system, as shown in Figure 3.

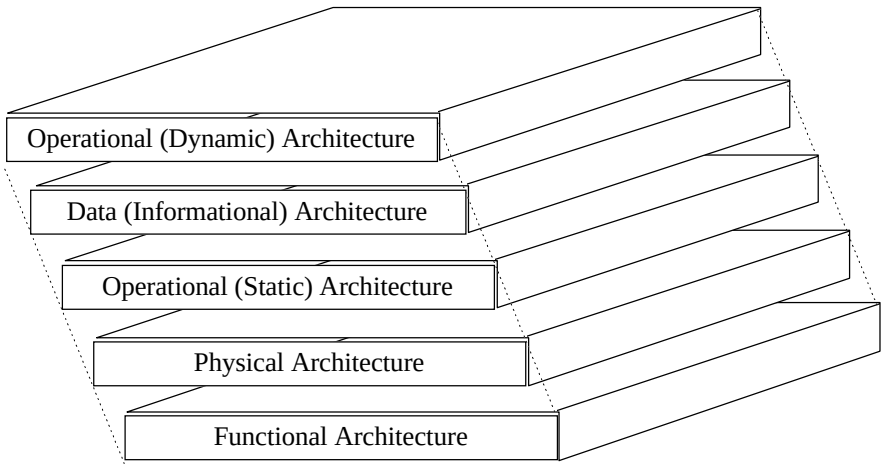

Figure 3. Operational Architecture—As a System of Layers

In the following sections, each of the individual layers, or architectures, of the Operational Architectures Model is discussed as is the underlying operational concept. The goal here is not to make system or software engineers of military planners, but to introduce the concept, construct, and thought process used in system modeling so they can properly apply information warfare analytical techniques.

Operational Concept

Every system has a purpose. The operational concept is the overall objective of the system—its purpose. It describes how the system will work and what it will do. This is

the foundation that allows one to tie the functional, physical, and data architectures together and develop the operational architecture.

Functional Architecture

The functional architecture of a system is modeled using the $IDEF_0$ method and is a structured representation of the functions of a system and the information and objects that interrelate those functions. To describe the functional architecture modeling, requires the introduction of three concepts—a function, functional modeling, and functional decomposition of a system.

A function is an abstract element of behavior which is not specific to the means of implementation. In other words, functions are the things the system does, considered without regard for the means by which it accomplishes them (i.e., which physical systems it may employ to accomplish its functions). Since functions are what the system does, they are described by an active verb phrase.

Using the $IDEF_0$ method, functional modeling is done by creating diagrams of system functions (boxes) and the interfaces between them (arrows). The position at which the arrows enter or leave the box conveys the role of the interface (see Figure 4).

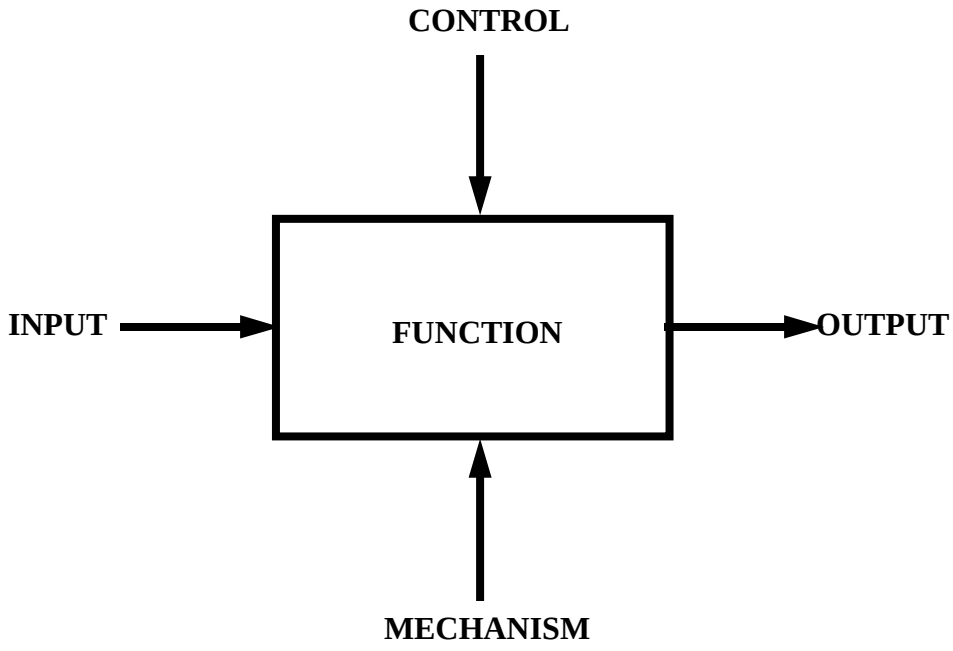

Figure 4. IDEF$_0$ Method[8]

Arrows represent objects or information needed by or produced by the function. They are labeled with a noun phrase written beside the arrow. Arrows do not represent flow or sequence. Input arrows show the types of objects or information needed to perform the function. Output arrows show the objects and information created when the function is performed. Control arrows describe the conditions or circumstances that govern the function. Mechanism arrows indicate persons or devices which carry out the function (i.e., the physical architecture).

The IDEF method starts by representing the whole system as a simple unit—a box with arrow interfaces to functions outside the system. Since the single box represents the system as a whole, the descriptive name written in the box is general and is based on the operational concept which defines the system's overall function. At this level, the arrows

represent inputs and outputs from the environment or the context in which the system exists.

In the next step of $IDEF_0$, functional decomposition, the box that represents the system as a single function, is detailed on another diagram with boxes connected by interface arrows. These boxes represent major subfunctions of the parent function. The decomposition reveals a complete set of subfunctions, each represented as a box whose boundaries are defined by interface arrows (see Figure 5). Each of these subfunction boxes may be similarly decomposed to expose even more detail. A function is always divided into no fewer than three, but no more than six subfunctions, thus ensuring enough, but not too much detail is introduced. Each box in a model is shown in precise relationship to other boxes by interconnecting arrows which illustrate the interfaces between the subfunctions. Each subfunction box's interfaces, taken together, define that subfunction's environment or context.

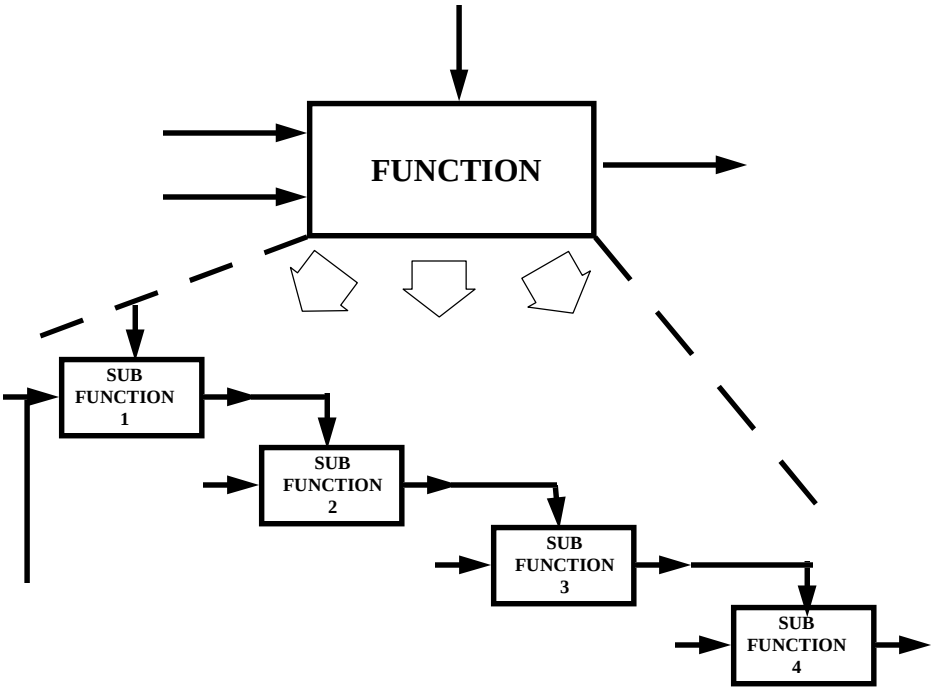

Figure 5. Functional Decomposition of a System[9]

Physical Architecture

Having defined the functions, or what a system does, one must now examine the means it uses to accomplish them. This is the system's physical architecture. In essence, for information systems, this is simply a laundry list of physical systems used to accomplish one or more of the system's functions. The physical architecture has no individual IDEF reference, but it constitutes the mechanisms referred to by arrows on the bottom of the boxes in $IDEF_0$.

Operational (Static) Architecture

Once one has modeled the system's functions and examined its mechanisms, the mechanisms are overlaid on the functions. In other words, the planner now matches

physical architecture with each of the functions. The result is the Operational (Static) Architecture, depicting the "what" and "how" of the system at rest.

Data (Information) Architecture

This section presents a simplified version of the $IDEF_1$ method. This simplification stems from the fact that it is not the authors' intent to turn information warriors into system engineers. In addition, the information warrior will not have the time nor the level of detailed information required for the full application of $IDEF_1$. Finally, the information warfare campaign planner simply does not need the volume or degree of analysis offered by full application of the $IDEF_1$ method. What is presented here is based on the underlying concepts of that method, but with reduced detail and selective application.

Planners need to look at information in a system to understand it, target it or protect it, and predict the effects of their actions. This understanding requires knowledge of the form and format of information in a system as well as the rules governing both form and transmission. However, information in the system is extremely complex. Systems may be huge, the different elements of data vast, and the rules obscure. For a good understanding without bogging down in unnecessary complexity, it is essential to reduce how much of the system must be examined in full detail.

Thus, the first step for planners examining the data or information architecture is to focus on the previously identified functions and the links between them. The planner's purpose is to identify potentially lucrative targets in the information architecture. Therefore, what the planner is looking for at this stage is information concentration.

A functional node may have large numbers of inputs coming into it, but fewer going out. For example, a warfighter begins with the function of "survey" in which he or she attempts to determine the situation on the battlefield. To do this, there may be information inputs from a large number of different sensors and surveillance systems. These inputs may then be distilled into a smaller number of outgoing situation reports of various types. The next function a warfighter must perform is to assess, or make sense of these reports. At this point, various pieces of situational information are merged with others for a more holistic view. Historical information may also be added now along with analysts' experiential information to result in an assessment of not only what is going on, but what it means. This results in an even smaller number of assessment products flowing to a commander, who makes a decision on what must be done. This decision is incorporated into a directive which also includes a distilled version of the assessments that were received. This directive now goes out to the control function in the form of a single message. At this point, information is highly concentrated. However, from the control function, the information flows to the execute function. Since execution can take many forms involving many different systems, at this point the information may begin to disperse somewhat into messages tailored for different elements of the execution function. In this example, the information flow from the command to the control function is the most highly concentrated, containing the distillate of a great deal of other informational flows. For sheer efficiency and maximum effect, it represents an excellent potential target meriting additional scrutiny.

Having identified one or more concentrations, planners must examine them more closely. Each one is made up of building blocks called entities. Entities can be physical

or abstract. For example, weapons systems, people, messages, and computers are physical entities. Abstract entities include such things as, in business, a complaint. It has no physical existence but it is an entity within the system. Each entity is uniquely identified by the series of properties it possesses, called attributes. Of importance to the information warrior, each entity has relationships to other entities both within and without the function and even the system. (see Figure 6) Only by identifying all of these relationships can one amass the knowledge needed to decide what entities to target, to select a method of attack, and to predict the effects.

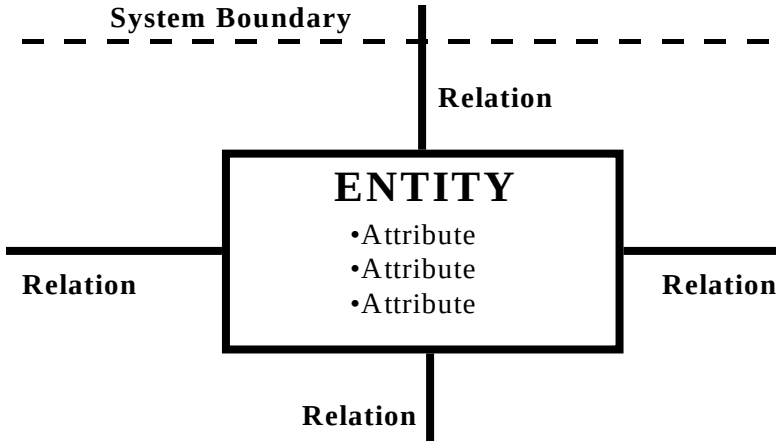

Figure 6. Information Model Format[10]

In information warfare, it is especially important to understand all these relationships because an attack on an information target could have unintended consequences. For example, an entity in an execute function may be the abstract entity called "navigation." This entity may have relationships that extend to a system of navigational satellites known as the Global Positioning System (GPS) as well as to a myriad of tanks, airplanes, and ships in the theater of war. To prevent accurate enemy attacks, an information

warrior may consider targeting the ability of the enemy's weapons to navigate, and may choose to do so by altering the navigational signals being supplied by GPS. Although this would indeed accomplish the objective, it could also have the unintended consequence of causing an airliner to crash. Careful examination of the navigation entity would have revealed a relationship to more than just military equipment and would have shown the planner the full effects of his or her actions.

Understanding a system requires one more element to allow accurate prediction of effects—time. This is captured in the final layer of the Operational Architectures Model.

Operational (Dynamic) Architecture

The final step in the Operational Architectures Model is to examine the system one is analyzing, using the $IDEF_2$ method, to gain an understanding of how the element of time affects it. The performance of the system is assessed in terms of its effectiveness and efficiency in converting system inputs into system outputs. By doing this, one acquires a grasp of the system's performance when in use—what it does and how fast it does it when the "switch" is turned on. This is a critical understanding for the information warrior because one of the goals of information warfare is to get inside an enemy's informational cycle by slowing it down or speeding up one's own. Thus, time is a major consideration in planning a campaign.

To understand system performance, the $IDEF_2$ method requires the planner to assess four considerations which, when combined, provide a dynamic view of the system. These four considerations, referred to as submodels, are Facility, Entity Flow, Resource Disposition, and System Control. This approach offers the advantage of breaking a large system into smaller components, permitting the planner to focus attention on a few details

at a time.[11] System engineers employing this method would take these submodels to much greater levels of detail than is required for a campaign planner. For the purposes of this campaign planning method, it will be adequate to address each of these submodels as considerations for the planner which will at least provide him or her with a reasonable impression of the system's performance. The discussion of each submodel will employ the example of a petroleum product pipeline network for added clarity.

The first submodel to be considered is the Facility Submodel. The $IDEF_2$ manual offers the following description:

> The $IDEF_2$ Facility submodel describes the resources which are used by the system to produce the final products or information. These resources may be physical, logical, or cognitive. Physical resources are any physical components of systems such as people, machines, and materials. Logical resources are any logical components of systems which determine their operation, such as computer software or manufacturing procedures. Cognitive resources are those resources which are required for thought processes such as experience and creativity.[12]

What this represents for the campaign planner is an organized approach to the common sense notion that to understand how a system works, one needs to understand who and what it has to work with, how these things operate, and what kind of ability it has to draw on. In the example of a petroleum pipeline network, this represents pipes, tanks, pumps, filters and valves. It also represents pipeline engineers—both their numbers and their knowledge and experience levels. Finally, it represents the distillation and storing processes the petroleum products have to pass through. Much of the work relating to this was done earlier, when the physical and informational architectures of the system were analyzed. The goal of the information warfare campaign planner here is to consider each of these elements and to thereby obtain an impression of how the physical,

logical, and cognitive resources available to the system affect its efficiency and performance. One need not quantify these considerations to obtain this level of understanding; for the information warrior they are simply that—considerations.

The next submodel to consider is the Entity Flow Submodel. According to the $IDEF_2$ manual:

> The $IDEF_2$ Entity Flow Submodel is the means by which the flow of products or information through facilities is described. An entity may be real or conceptual. Examples of entities are products or information which are operated on or produced by the system being modeled. It is in the Entity Flow Submodel that the actual processing of products or information is described. The activities which are performed as well as the decisions regarding alternate flow of entities are also described.[13]

Again, this is simply a formalized call for the common sense requirement to understand how things move through the system in order to understand how efficient it is. In the petroleum pipeline example, there are several different petroleum products which flow through this network such as oil, kerosene, and gas. Each of these is an entity. In this submodel, one must consider how fast these entities can flow through the pipes—what is the length and diameter of the pipes, how many elbows and valves are encountered, how viscous are the entities, etc. In another example, if an entity called Air Tasking Order (used to task military aircraft to execute operations) has to pass through large numbers of systems, perhaps requiring format translation from one system to the next, and cross numerous desks before arriving at its final destination, one would reasonably expect potentially significant time delays when compared to a more streamlined system. As the manual points out, the planner must also consider alternate paths that an entity might take through the system. In a pipeline, this is the connecting pipes which could be used to bypass a blockage, for example. One must also assess

storage capacities at various points in the system, which may serve to provide the ability to surge or function despite a rupture in the upstream pipeline, thus acting as a temporary alternative. In the Air Tasking Order example, it may be that in times of crisis several systems and desks it goes through in routine operations are bypassed. This is a crucial consideration for anyone trying to understand and perhaps exploit a system's speed (or lack thereof).

The third submodel of the $IDEF_2$ method is the Resource Disposition Submodel. According to the $IDEF_2$ manual:

> The $IDEF_2$ Resource Disposition Submodel is used to describe the disposition of resources when they become available. A resource in $IDEF_2$ is any part of the system which must be present to perform an activity.[14]

In this submodel, the information warfare planner must consider what critical resources are available and how efficiently they are used. For example, a system performing the surveillance function may be attempting to obtain imagery of a particular site. To do this, the system employs reconnaissance aircraft and orbiting satellites. Here, the planner considers how often and how quickly each of these resources is available to accomplish the task. The aircraft, for example, may be unavailable due to maintenance or battle damage. If it is available, it may take several hours to task it, get it to the site, and bring it back. The satellite may only pass over the site twice a day and it may be busy looking at other, more critical, sites. Going back to the petroleum pipeline example, certain branches may be occupied transporting kerosene and not available for other petroleum products to move. Other parts of the pipeline may also be under repair. If a sudden order for gasoline is received, pipeline availability will determine if the order can be filled at the same time the kerosene order is moving through the system, or if the

kerosene must be interrupted or the gasoline delayed. What critical resources are available to a system and how they are employed is an important consideration for understanding the speed and efficiency of system performance.

The final submodel for the information warrior's consideration is the System Control Submodel. Per the manual:

> The fourth $IDEF_2$ submodel is the System Control Submodel which describes the occurrences of activities which control but do not prescribe the flow of entities. Situations handled by the System Control Submodels include the breakdown and repair of resources, the arrival of entities, the alteration of resource capacities, the initiation and termination of shifts and the alteration of job priorities.[15]

The previous submodel considered the availability of resources. Here, one considers how those resources which are available are controlled. Returning to the pipeline example, the overall throughput of the system is determined by its structure and availability, both of which were considered already. In this submodel, the planner is considering the control of the available resources and throughput. In the case of the sudden receipt of an order for gasoline while the pipelines are occupied moving kerosene, the planner now assesses how the system establishes which product will have the higher priority. This control may take the form of valves being opened and closed, unusable pipeline segments being repaired, maintenance on other pipeline segments being postponed, workers being instructed to work overtime, etc. The speed with which controllers respond to an input, the range of options available to controllers, and the speed with which the system responds to the controllers must be understood by anyone attempting to comprehend the dynamics of the system.

The four submodels, taken together, provide a range of considerations for the information warfare planner which result in an understanding of the system being analyzed that goes beyond its structure and offers insight into its performance under various conditions. Speed and efficiency considerations address the time element in the system. These considerations complete the culminating step of the Operational Architectures Model, the Operational (Dynamic) Architecture.

Summary

As in any campaign, the most useful way to gain the understanding necessary to attack or defend is to view the enemy and oneself as systems. This is most effectively done by a modeling method which offers a structured approach to viewing the system. There are a variety of models available for viewing systems, each of which, by the questions it forces one to answer, brings to the fore different aspects of the system being analyzed. The Operational Architectures Model, employing IDEF methods, is uniquely useful to the information warfare planner because it provides an effective tool for identifying the flow of information through a system. As a result, it provides the planner with an understanding of the system's purpose, functions it must accomplish to achieve its purpose, mechanisms it employs to achieve its functions, and its efficiency/effectiveness. Armed with this understanding, the planner can now move on to other aspects of his or her planning.

Notes

[1] Mendel, William W. and Tooke, Lamar. Military Review. January 1993.

Notes

[2] Luchsinger, Vincent P. and Dock, V. Thomas. "The Systems Approach—A Primer," 1.

[3] Ibid.

[4] Air Force Wright Laboratory. "Integrated Computer-Aided Manufacturing (ICAM) Architecture Part II, Volume VI-Dynamic Modeling Manual (IDEF2) TR-81-4023. Wright Patterson AFB, Ohio, June 1981, 8.

[5] Warden, J.A.. "The Enemy as a System." ACSC Strategic Structures Coursebook Volume II, 437-441.

[6] Integrated Computer-Aided Manufacturing (ICAM) Architecture, 3.

[7] Air Force Wright Laboratory. "Information Integration for Concurrent Engineering (IICE) IDEF3 Process Description Capture Method Report." AL-TR-1992-0057. Wright Patterson AFB, Ohio, May 1992, xi.

[8] Air Force Wright Laboratory. "Integrated Computer-Aided Manufacturing (ICAM) Architecture Part II, Volume IV, TR-81-4023. Wright Patterson AFB, Ohio, June 1981, 17.

[9] Ibid. 13.

[10] Air Force Wright Laboratory. "Integrated Computer-Aided Manufacturing (ICAM) Architecture Part II, Volume V, TR-81-4023. Wright Patterson AFB, Ohio, June 1981, 37.

[11] Dynamics Modeling Manual-$IDEF_2$, 17-18.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

Chapter 3

Applying the Operational Architectures Model

The previous chapter provided a model and associated methods the information warfare planner can use to analyze systems. The advantage of the Operational Architectures Model for the information warrior at any level of conflict is its ability to highlight information within a system. It reveals the purpose of information in the system, how it is handled, and how efficiently it moves. The model is also useful for identifying vulnerabilities in the flow of information in a system. Unfortunately, at first blush the model appears rather complex. In view of this, it is instructive to apply the model to a relatively familiar system. This chapter will do that, employing the Operational Architectures Model to analyze a notional Joint Force Air Component Commander (JFACC).

The US military is divided into geographic combatant commands headed by a Commander in Chief (CINC). In combat operations, the CINC will normally appoint a Joint Force Commander (JFC), who will in turn appoint a commander for each force component (land, air, sea, special operations). The JFACC is the air component commander. In the Persian Gulf War, the CINC was General Schwarzkopf, Commander in Chief of US Central Command. He also acted as the JFC. His Joint Force Air Component Commander was Lt Gen Horner. This example was selected for analysis

because it is relatively recent and the Desert Storm air campaign was so prominent most readers will have at least some familiarity with how a JFACC functions. Therefore, it will serve as a concrete example of how a planner can use the Operational Architectures Model to analyze a system for information warfare purposes, identifying critical nodes and enabling the application of tools from the information warfare arsenal to attack or defend these potential targets.

Operational Concept and Functional Architecture

The first step in applying the Operational Architectures Model to a JFACC system is identifying its overarching purpose. This purpose becomes the underlying operational concept for the entire model.

Having identified the operational concept of the system, one can now identify its functional architecture, including inputs and outputs, controls, and mechanisms. One begins with the operational concept, i.e., the purpose for which the JFACC exists, then decomposes that function into its primary subfunctions, as illustrated in Figures 4 and 5 in the previous chapter.

In the case of a JFACC, the function is to organize and employ airpower in a unified fashion to accomplish military objectives in support of a JFC's overall campaign—in short, to conduct a theater air campaign. (See Figure 7.) Control inputs to the system are represented by a hierarchical chain of command leading from the National Command Authority (NCA) to the CINC to the JFC and then to the JFACC. This control mechanism dictates the strategic objectives and desired endstates from which the operational objectives are derived. The JFACC then employs airpower to help obtain the

operational objectives. Contextual elements beyond the system's control (environment, political situation, international factors, socio-cultural factors, economic factors, and leadership factors) also represent controlling elements. Inputs to the JFACC system include the operational art elements which shape the JFACC's military options (logistics, technology, information, targeting science, deception, and measuring success). The mechanisms are the physical means by which the JFACC carries out his or her purpose. These are examined in detail as the system's physical architecture. Finally, the output of the JFACC system is an operational air campaign.[1]

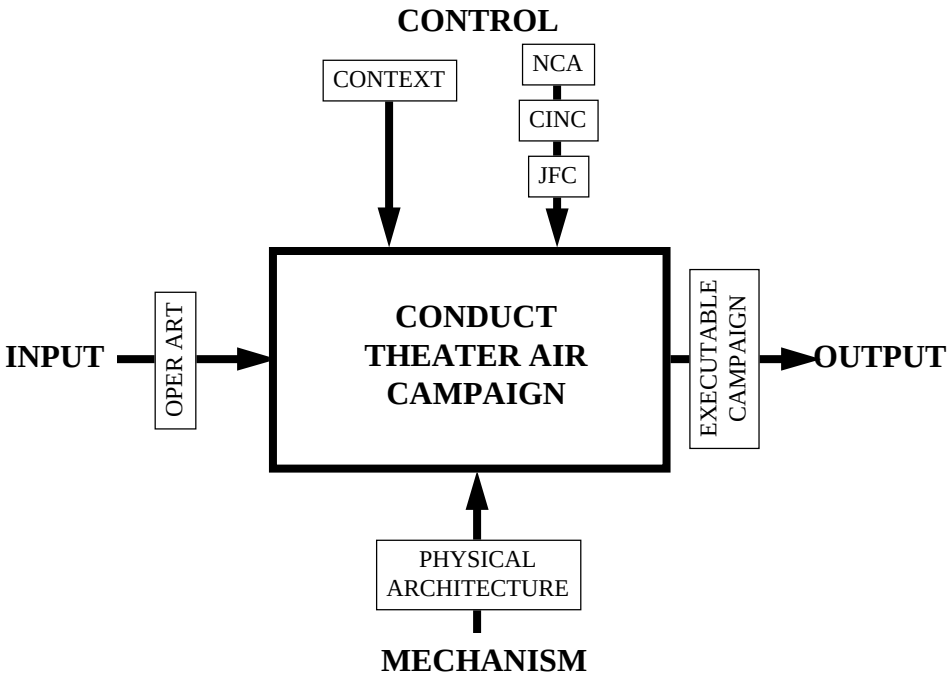

Figure 7. JFACC Function

The planner's next task is to perform a functional decomposition of the JFACC system. As one would expect, systems designed to accomplish the same general purpose will have to accomplish the same subfunctions as well. Thus, systems designed for the purpose of applying force to achieve military objectives can be decomposed in the same

way. This, of course, has been observed by many. For example, one of the most well-known models of military systems' subfunctions is John Boyd's OODA Loop. According to Boyd, every system performs four functions: Observe (see what the situation is), Orient (analyze what has been observed and give it meaning), Decide (figure out what to do about it), and Act (execute operations). It is a loop because once one has acted, one must observe the new situation, and so on.[2]

In applying the Operational Architectures Model and the IDEF methods to analyze a military entity for information warfare, one should employ a 5-function decomposition rather than Boyd's four functions. These functions are: survey, assess, command, control, and execute. There is an advantage in using these, rather than the OODA loop, as the subfunctions of a military system for information warfare analysis. In Boyd's model, the decision phase represents the military functions of both command and control. In essence, the command and control functions are thought of together, their lines of distinction being blurred to the point of invisibility. For the purposes of this analysis, a distinction is necessary because key informational interchanges occur between the two functions and the intent of each function is quite different. By breaking the decision phase into its components, the function and flow of information in this critically important area is more readily exposed. The JFACC's functional decomposition is illustrated in Figure 8.

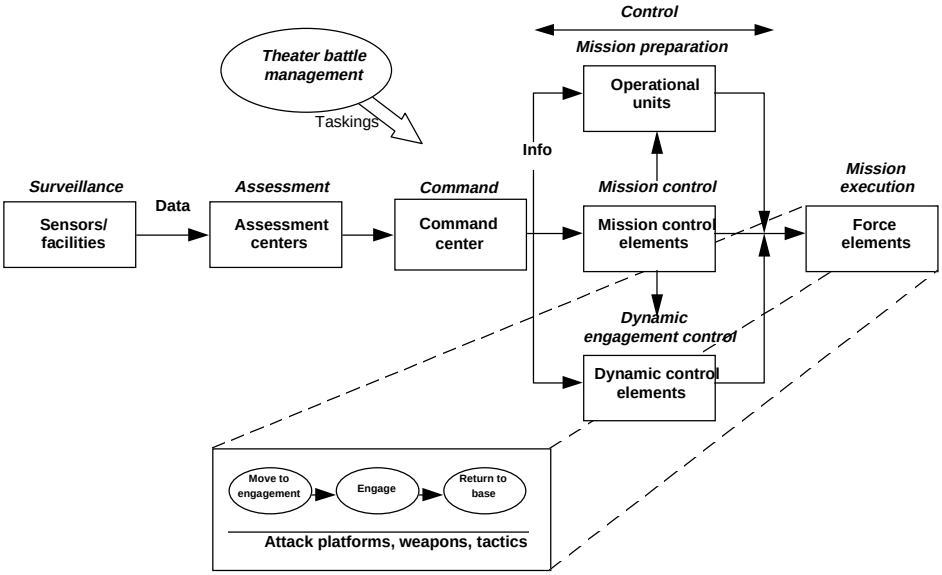

Figure 8. JFACC Functional Decomposition[3]

As with the overall system, each subfunction has a purpose which must be identified. What information does the system need to survey in order to conduct an air campaign? At a minimum, the commander must have total situational awareness, defined as "…awareness of the enemy disposition, capabilities, intentions, and vulnerabilities, as well as, pertinent information on one's own forces."[4] The information the system surveys is further clarified by objectives, the situation, and the environment. All of this information, once surveyed, must be assessed. The assessment function processes and analyzes the massive amounts of surveyed data to produce an integrated picture of the battlespace. This picture is provided to the command function in a useable format upon which the JFACC can base decisions. In the command function, the JFACC and his staff must review and further analyze the assessed data. The analysis, in this function, consists of identifying potential targets which will meet military objectives and aligning air assets against them. Those targets which the JFACC believes will achieve the objectives

become a part of the overall air campaign plan. The next functional area is control. In this step the JFACC disseminates his or her decisions on targets and weapons systems, provides mission planning guidance, and oversees the actual conduct of the operations. In the last functional step of this model, tasked units execute assigned missions against designated targets. Obviously, there is some overlap in the timing of these functions, but each function is essential to the successful function of the system as a whole.

Physical Architecture

Once the JFACC's functional architecture has been described, the planner must identify the physical mechanisms which inhabit the system. As noted previously, these systems represent the mechanisms the JFACC system uses to accomplish its functions. Table 1 shows the physical systems available to the JFACC during the Persian Gulf War.

Table 1. JFACC Physical Architecture

Surveillance Assets	Assessment Assets	Command & Control Assets	Execution Assets
National Assets	Checkmate	AWACS	F-111, 15E, 16,
SPOT (French)	Black Hole	JSTARS	117A
Landsat	Fusion Centers	RC-135	TLAM
RF-4		CAFMS	F/A 18
TR-1		C4I Systems	A-6/7
JSTARS		Coalition C4I	B-52G
AWACS		Systems	Coalition Aircraft
Other Intel Sources			

Operational (Static) Architecture

The physical architecture, when combined with the functional architecture, is the JFACC's Operational (Static) Architecture. (see Figure 9)

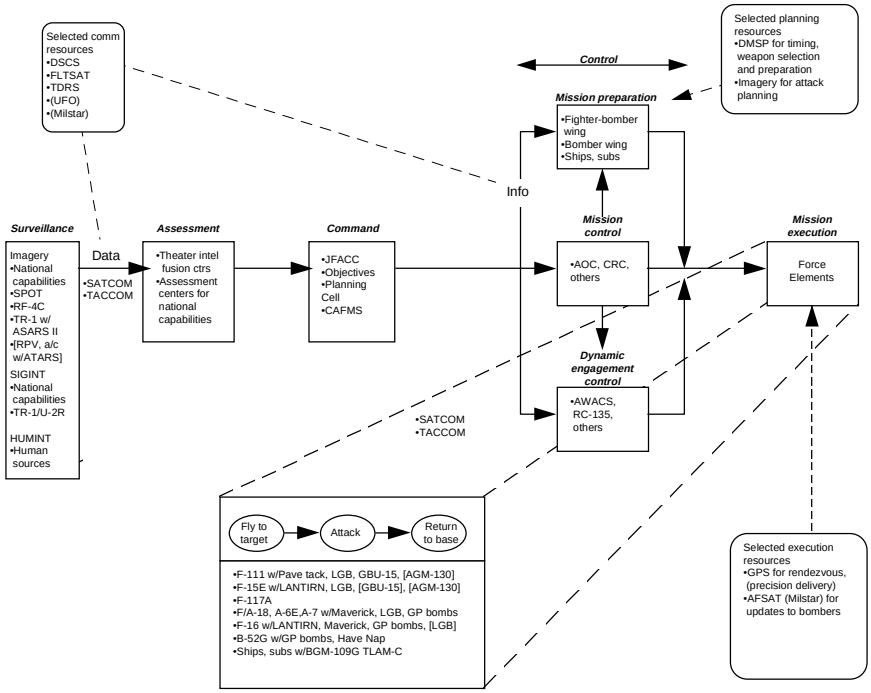

Figure 9. JFACC Operational (Static) Architecture[5]

Data (Information) Architecture

The next step in the model is to analyze the JFACC's data and information architecture. It is the planner's goal here to understand the interdependencies within the JFACC's information sphere. As noted in the previous chapter, this analysis should be conducted on those points which represent highly concentrated information. In the JFACC system, the most highly concentrated point in the information flow is from the command function to the control function (see discussion of this in the previous chapter). This concentration represents a point of vulnerability which must be protected or can be attacked, depending on the planner's objectives. Having identified an information concentration, the next step is to use the $IDEF_1$ method to identify specific entities which comprise it and their relationships to other entities.

In the JFACC example, an Air Tasking Order (ATO) is an important entity comprising the concentrated information flow between command and control. This is a formatted message product which matches units and weapon systems with targets, ordnance, timing, and other specifics of mission assignments. Using $IDEF_1$ modeling terms, the ATO is considered a physical entity, its form and format constituting its attributes. This entity has linkages to the command, control, and execute functions; it also has relationships with other information produced in these functions. The ATO as an entity, along with some of its most important relationships, is depicted in Figure 10. By understanding an entity and its associated relationships, a planner can determine its suitability as an information warfare target. He or she can also determine what effects, both intended and unintended, will result from targeting the entity. Of equal importance, an information warrior can determine interdependencies among entities. Targeting entities with large numbers of dependent relationships could yield the most lucrative targets.

Figure 10. Air Tasking Order Data (Informational) Model

Operational (Dynamic) Architecture

The last step in Operational Architecture Modeling of the JFACC is analyzing the system's function when the time element is introduced. This analysis sheds light on the efficiency and effectiveness of the system. In effect, it allows the planner to comprehend the system's inherent ability to cope with what Clausewitz referred to as fog and friction. The analysis is accomplished by applying the four considerations, or submodels, introduced by the $IDEF_2$ Method. The four submodels are: Facility, Entity Flow, Resource Disposition, and System Control. (See Figure 11.)

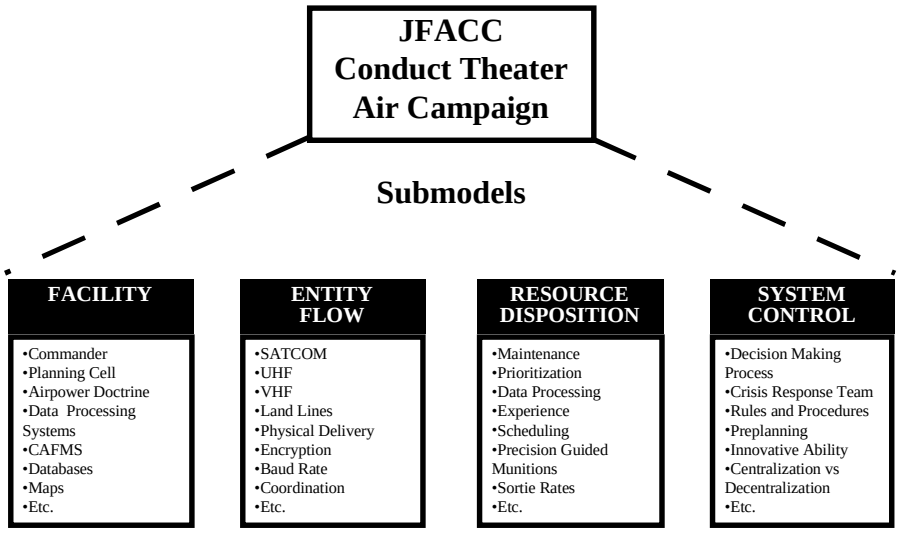

Figure 11. JFACC Submodels

The Desert Storm air campaign offers an excellent example of the utility in considering the time factor when analyzing a system. During that war, the ATO product was initiated in a planning cell called the "Black Hole" (an important part of the Facility Submodel). The Black Hole planners used a variety of means to circumvent perceived roadblocks to obtaining timely intelligence information and damage assessments. Nonetheless, they often felt these elements of the information system were too slow and unresponsive to the exigencies of mission planning. This interfered with the planners' ability to decide exactly how to service some targets, or to determine whether targets had been adequately affected. Against a more sophisticated and aware opponent, this could represent a targetable vulnerability.

Another vulnerability, related to time, was encountered, although never exploited by the stunned Iraqis. That vulnerability lay in the time required for the creation and distribution of the daily Air Tasking Order. After targets were picked to meet the next day's objectives, the ATO was created and transmitted using the Air Force Computer-

Assisted Force Management System (CAFMS) (a facility element).[6] Once received, it gave detailed directions on the numbers, type, and use of the weapons systems available for that day's sorties (resource disposition). Finally, the control functions (Airborne Control Element and Air Operations Centers) use the ATO as the sheet of music for the airpower concert (system control) while air weapons systems executed the specified missions. On a good day during the Persian Gulf War, this cycle took 28 hours from the conception of the targeting list to the execution of the ATO.

Problems occurred early in the conflict which prevented timely distribution of the ATO to all joint forces. Most notable was the Navy's inability to electronically download the ATO. The Navy's equivalent ATO system was not compatible with the format and volume of the JFACC's Air Force-styled ATO. This problem was initially solved by transporting a floppy disk with the ATO on it via helicopter to the fleet. Later, communication equipment aboard ship was changed to accept the ATO transmissions. Although Iraq never exploited this, an information warfare-savvy opponent could have used this vulnerability to his advantage.

As the ATO example demonstrates, it is only when the time factor is added to the Operational (Static) Architecture of the JFACC that certain critical information warfare vulnerabilities become apparent. Clearly, moving through the Operational Architectures Model and arriving at an understanding of a system's Operational (Dynamic) Architecture allows the most thorough analysis and reveals the system's informational vulnerabilities. From this knowledge, a planner can successfully devise methods to attack or defend the system. The following chapter will discuss specific tools for the information warrior to employ in this endeavor.

Notes

[1] *War Theory Coursebook,* "Air Campaign Planning," Air University Press, Maxwell AFB AL, 14.

[2] David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, Air University Press, Maxwell AFB AL, February 1995, 16.

[3] Department of the Air Force *Operational Concepts Primer for USAF Planning*, DCS for Plans and Operations, USAF, 1 March 1995, 2.

[4] *Report of the Defense Science Board Summer Study Task Force on Information Architecture For The Battlefield*, Oct 1994, pub by Office of the Under Secretary of Defense For Acquisition & Technology, Wash DC, 6.

[5] *Operational Concepts Primer for USAF Planning*, 8.

[6] Alan D. Campen, editor, *The First Information War*, article by Joseph S. Toma, "Desert Storm Communications," AFCEA International Press, Fairfax, VA, 1992, 4.

Chapter 4

Information Warfare Tools

The previous chapters provide the foundation for modeling an opponent's or even one's own information processing systems. Modeling is not enough to conduct an information warfare campaign. Practical tools and techniques must be employed to prosecute the campaign. This chapter will examine these.

To conduct an information warfare campaign, the same five subfunctions must be accomplished which were previously discussed. Figure 12 provides a simplified depiction of these subfunctions. The discussion which follows will focus attention on the tools and techniques used by the information warrior in accomplishing each of these subfunctions in the context of a military campaign.

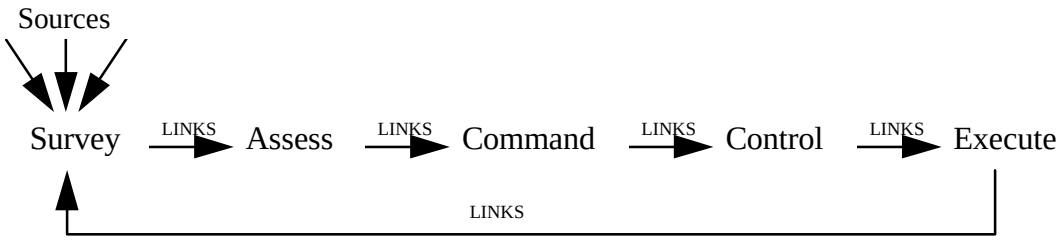

Figure 12. Five Subfunctions

Survey

Survey is the first subfunction. This step includes the accumulation of data covering

one's opponent's information system for the planners to employ the Operational Architectures Model. Assets the planner can use to gather this information range in sophistication from a multimillion dollar satellites to an agent working undercover to open source information from the Internet or the local library.

Information collection is performed through seven primary means. They are imagery intelligence, human intelligence, signals intelligence, measurement and signature intelligence, technical intelligence, counterintelligence, and open source intelligence.[1] All the information used to write this chapter was obtained, with little difficulty, from open sources. Open source information is widely available and can be used during the initial analysis process, then fleshed out at a later date with more accurate and validated information from the other sources listed above.

Depending upon one's needs and the level of conflict at which one is operating, surveys can range from tactical to strategic in scope. For a strategic-level survey, the area of interest can encompass entire nations or regional areas. In an operational or a tactical environment, the areas of interest may be an limited to a country, a city, or even a battlefield. During Desert Storm, for example, coalition forces required both strategic and operational level intelligence covering the electromagnetic spectrum. They obtained this information via the space assets listed in Table 2, to which they had varying degrees of access.

Table 2. Space Surveillance Assets During Desert Storm[2]

Satellite	***Function***	***Country***
Military		
Defense Support Program (DSP)	Early warning/thermal IR	US
Defense Meteorological Satellite Program (DMSP)	Weather observation	US
RORSAT	Radar ocean reconnaissance	Russia
EORSAT	Elint ocean reconnaissance	Russia
USSR Reconnaissance	Optical reconnaissance	Russia
ALMAZ	Radar	Russia
Civilian		
Spot	Earth observation—visible	France
Landsat	Earth observation	US
GOES	Meteorology	US
NOAA	Meteorology	US
METEOR	Meteorology	USSR
OKEAN	Oceanography/radar	USSR
RESURS-F	Earth observation/photo	USSR
RESURS-O	Earth observation/thermal & visible	USSR

The overall picture this mix of systems of this sort is capable of providing to the information warrior is quite broad. The capabilities of thermal detection satellites such as DSP and Landsat range from near-real-time detection of missile launches to determining where wetlands are in the desert. Radar satellites provide all weather surveillance capabilities, and commercial satellites provide critical background information products. For example, the combining of commercial SPOT and LANDSAT satellite outputs with the use of a commercially available software program produced detailed road maps of Kuwait for the coalition forces.

Stepping down one notch to air-breathing assets, traditional overflights by reconnaissance aircraft provide theater and tactical awareness. Dedicated systems such as the Joint Surveillance and Target Attack Radar System (JSTARS), Airborne Warning and

Control System (AWACS), and U-2s provide theater and tactical level surveillance, whereas, RF-4 systems provide tactical level surveillance. Because of the direct link back to the theater commander, this method of data collection is usually more timely than space assets. Data can also come from innovative use of other air-breathing systems. For example, the Iranians use the air-to-air radars of the F-14 Tomcat fighter to provide a "miniature AWACS" tactical picture during the Iraq-Iran war.[3]

Finally, ground capabilities to acquire the information required in the survey step include traditional and less traditional methods. Traditional methods include human intelligence, technology intelligence, open source intelligence, electronic eavesdropping, etc. A non-traditional source is now causing increasing concern, not only from the government, but within the private sector as well. This is the unauthorized entry into electronic data systems—"hacking" is another word for it.

Through computer hacking, it may be possible to enter an adversary's computer files and obtain detailed information on his or her capabilities, readiness, and even the financial status of the government. The tools for hacking are inexpensive: a personal computer and a modem are all it takes. With these simple tools, a hacker has the potential to access any other computer which has a modem. What is truly unique in this is that it can be done by a person on a personal computer located thousands of miles from the target.

Assess

The second subfunction the information warrior must accomplish is to assess the information collected in the previous step. The survey data is now processed and

analyzed. A term used to describe this process is "information fusion," the combining of information into a battlespace picture which the information warrior can use.[4]

To be assessed, the information warrior must begin by moving the information from the survey function to the assessment function. Some avenues for movement of information into and out of the assess function are radio, microwave, satellite downlinks (radio or microwave), commercial and military phone systems (secured & unsecured), fiber optics, pilot debriefs, papers, facsimiles, message traffic, and courier. In the information age, the means overwhelmingly favored by those who possess the ability is electronic transfer of data.

As the distance between sender and receiver increases, so does the likelihood that satellites will be the preferred mode of transmission. In a period of high demand, both commercial and military satellites are used. During Desert Storm, for example, 22% of military traffic went over commercial satellites.[5] Satellites can even be used to transfer data to other satellites, such as the Tracking and Data Relay Satellite System (TDRSS), to achieve worldwide coverage.

In the case of surveillance satellites, these systems are limited by their ability, or lack of it, to process data. It takes a tremendous amount of computing capability to produce meaningful data or pictures from the raw data coming from their sensors. This amount of computer capability takes space, and in satellites, space is at a premium. Therefore, the raw data is relayed via a ground-based down-link site to analysis centers for processing. Processed data then enters the assessment function to be analyzed by human and computer based interpretation methods. When analysis is completed, it is reported to the command and control function over the same lines of communications previously

described.

Once received, the data is evaluated by intelligence analysts to determine its meaning. Assets involved in this process include such things as specialized software, computer data bases, and imagery viewers.

Command

The command function receives the battlefield picture from the assessment function, conducts planning, and determines courses of action. In this step, information warriors employ manual or automated planning systems and target data bases to produce an overall information warfare campaign. They also create the campaign's increments, whether daily, hourly, or other. These increments include matching specific information warfare tools to centers of gravity identified in the assessment phase.

The information campaign plan is now transferred to the control function which oversees its implementation.

Control

The control function analyzes received tasking orders, readies assets, responds to the threat and situational changes, and reports the results back through the chain of command. There are very few assets dedicated directly to the execution of information warfare. Instead, the assets which are employed will be drawn from those belonging to the land, air, and sea components. Thus, the control function will normally be performed via the control mechanisms of the components.

Thus, the tools information warriors use to control execution of the campaign will include a mix of assets such as AWACS, Aegis cruisers, and airborne, ground-based and

afloat control centers.

Both the command and the control functions use the communication avenues described earlier.

Execute

Execution in an information war includes two facets: information attack and information defense. Means for executing both offensive or defensive actions are broken into six sub-categories, each of which will be discussed further. Regardless of the method employed, the desired effect is to create a combination of "data overload" and "data starvation" in the adversary's information system which will degrade his battlefield picture, and to protect one's own system from these effects. A data overload occurs when a system cannot handle the information coming into it or flowing through it. Conversely, data starvation is when adequate inputs to the information system cease. These can be rapidly and efficiently achieved by simultaneous operations against a variety of different information points, a concept known as "parallel warfare."[6]

When a multitude of information points are attacked in parallel, two results occur in the information system. First, the disrupted points no longer provide information to the downstream functions and thus "starve" the parts of system they are connected to. Secondly, segments of the information system which are not disrupted now have to carry the existing load of the entire system, as well as the increased traffic flow from real or artificially induced disruption reports. This one-two punch can spell disaster for an unprepared adversary. But, how can the information warrior achieve this desirable effect?

As mentioned above, there are six categories of operations which can be employed to attack or defend information. The categories are:

1. Psychological operations—use of information to affect the enemy's reasoning
2. Electronic warfare—denies the enemy accurate information
3. Military deception—misleads the enemy about one's capabilities or intentions
4. Physical destruction—converts stored energy to destructive power
5. Security measures—denies information on military capabilities and intentions
6. Information attack—directly corrupts information without visibly changing the physical entity within which it resides.[7]

Before discussing each of these in detail, it is important to realize that some aspects of information warfare have been around for thousands of years. In addition, many of the principles of traditional forms of warfare apply as well to information warfare. Therefore, as the following discussion reveals, many capabilities to conduct elements of what we now call information warfare already exist. Some possible future capabilities will also be mentioned.

Psychological Operations

Psychological operations are currently being performed by systems such as the MC-130E Combat Talon I. During Desert Storm, the MC-130E flew multiple missions air-dropping and dispersing leaflets and it also air-dropped 11 15,000-pound BLU-82/B general purpose bombs. The use of psychological leaflets followed by a demonstration of strength proved to be very effective against the Iraqis.[8]

Could leaflets be used against the United States' forces? The likelihood of this form of psychological attack working against well educated and highly motivated forces seems slim, but other psychological weapons may be more effective. Consider, for example, the probable response of the public and allies to Cable News Network footage of a US Army platoon machine-gunning innocent civilians. With the rapid increase of quality

computer-generated images, it is conceivable that in the near future such scenes could be fabricated. Hollywood studios are now using this very process to create movies such as *Jurassic Park* and *Jumanji*. It is only a matter of time before counterfeit people appear on the screen. Aimed at the American need to maintain a reasonable level of public support for military operations, inherent to a democracy, such an attack could have very deleterious effects.

Electronic Warfare

Only in the past decade has information warfare begun to be seriously viewed as an important area in conflict, on the level of a separate campaign. The primary cause for this new focus is the exponential growth of computer-based systems. For this discussion, computer-based systems include anything which uses a microchip processor to perform it's function.[9] Based upon this definition, not only are the personal computers in your office considered to be computer systems, but so is the office's advanced electronic coffee pot. Why is this important? Because all computer systems have common requirements and constraints. Their performance is directly tied to electromagnetic fields, variations in power, environmental conditions, and quality of the associated software and hardware. One aspect of electronic warfare in an information warfare campaign concentrates on altering the computer system's electromagnetic environment.

One means to accomplish this is to use electromagnetic pulses (EMP). Pulses, such as from a high-powered radar, can destroy unprotected computer systems. Nuclear weapons have long been know to be huge EMP producers, but the global political environment and the morality behind using such weapons prevent their use by rational governments. Directed energy weapons which produce EMP without nuclear explosions

are now being discussed by futurists and are even reported to have been used in Desert Storm.[10]

Another aspect of electronic warfare is information denial through jamming an adversary's radar and other electronic systems. The EF-111A Raven is a premiere example of an electronic warfare platform; designed to provide electronic countermeasures support for tactical air forces, it can detect, sort, identify and nullify various enemy radar systems.[11]

Military Deception

Military deception is another means of information warfare which has been used for centuries. It can take the form of "leaked" military plans, or an amphibious landing to draw attention away from the main attack. In more modern times, inflatable aircraft, ghost tent cities, and press-on craters all help to confuse the collection sources of one's adversary and thus impact his decision-making ability.

Physical Destruction

When considering warfare, people often picture physical destruction as something like a B-52 flying over a target and dropping tons of dumb bombs. It is, but it is also much more. Precision-guided munitions such as the AGM-88A/B/C High-speed Anti-Radiation Missile (HARM), the AGM-65 Maverick, and the GBU-15 bomb, an unpowered glide weapon, can provide deadly accuracy in attacking information systems. During Desert Storm, the deep, hardened, command and control bunkers in Iraq fell prey to the laser-guided GBU-28. Made from old gun barrels, the GBU-28 can penetrate more than 100 feet of dirt or 20 feet of concrete.[12]

Another example relates to space-based information systems. These are hard to physically attack. But space assets all have a common thread—all downlink to ground stations. These ground stations can be easily damaged by cruise missiles, cutting power or communication lines, thereby effectively neutralizing space assets through destructive means.

Another potentially destructive tool for the future is the use of micro-electromechanical systems (MEMS). Research is ongoing to create micron-sized mechanical gears, pillars, and operational motors.[13] When these developments bear fruit, it is conceivable that millimeter- or centimeter-sized machines, e.g., robots, could be mass produced and introduced into a high value target to achieve some sort of destructive effect.

Security Measures

Security measures in information warfare range widely. The protection of a tactical telephone switch with sand bags is considered defensive information warfare. So is the use of computer passwords, operational security, communications security, and all those other security programs which make information gathering difficult, but not impossible. Other measures include the use of encryption systems such as the STU-III and the installation of electronic firewalls (a technique for preventing or controlling outsiders' ability to access internal systems) to ensure classified and other high-value information remains inaccessible to an adversary.[14]

Information Attack

Information attack, defined again, is the direct corruption of information without

visibly changing the physical entity within which it resides. Computer hacking is central to this category. This method of strategic cyber-attack represents part of what is new in the information realm—the ability to directly manipulate an adversary's information. The potential damage or gain from this area is staggering. For example, space assets are very difficult to directly to affect. However, what if a hacker or a disgruntled employee gained access to the satellite control system and directed satellites to shut down temporarily, to change their orbits, or even worse, to deorbit?

Closer to home, a computer system could be infected with a computer virus which, at a certain time or event, would erase all information on the hard drive. There are currently an estimated 3,000 different types of computer viruses in the world with the number increasing daily.[15] Their destructiveness is dependent mostly on what the computer contains or controls, the effectiveness of anti-virus programs, and what part of the computer operating system is targeted. In a sense, viruses can be thought of as an electronic weapon of mass destruction—indiscriminate and hard to control once released.

Survey

Having examined the execution function, the system then returns to the survey function. This constitutes a feedback loop to determine the effects of the execution and identify problems in the functions leading up to execution. Actual effects may not be those which were desired. For example, successful destruction of a critical communications link may have succeeded in preventing an adversary from receiving some information. However, if entity relationship analysis was not done properly, it may have had the unintended effect of destroying a cyberspace intelligence source because a

friendly hacker had already breached the link's security and was reading all the message traffic.

The survey after execution may also show unanticipated beneficial effects. In Desert Storm, the extremely successful use of HARM anti-radiation missiles not only destroyed radar sites (information gathering sites), but created an environment where the operators of fully functional sites refused to turn on their systems. Air Vice Marshall Bill Wratten, RAF, commented on this, stating, "Any anti-radiation missile, whether it gets a hard kill or whether it enforces switch-off, has achieved its aim." [16]

Summary

Information warfare is both a very old and a very new style of warfare. The desired effect remains the same—only the forms of information processing and tools to attack them have changed. The aim of this chapter was to provide a brief survey of representative systems and methods which the information warrior can use to conduct an information warfare campaign. When planning an information warfare campaign, a planner will likely have more resources available than were described here. Bearing in mind that each system and situation is different, the information warrior must match available resources to the vulnerabilities identified by the Operational Architectures Model to devise a successful campaign. A step-by-step method to accomplish this is described in the final chapter.

Notes

[1] *Joint Doctrine Capstone and Keystone Primer*, 25 May 1995, 21.

Notes

[2] *The First Information War*, Campen, 130.

[3] Ibid., 67.

[4] *Joint Doctrine Capstone and Keystone Primer*, 74.

[5] *The First Information War*, 139.

[6] *Firing for Effect: Change in the Nature of Warfare*, 3.

[7] Department of the Air Force, *Cornerstones of Information Warfare*, 1995, 5-6.

[8] USAF Fact Sheet 92-63.

[9] Air Intelligence Agency Briefing to Air Command and Staff College, 31 January 1996.

[10] *Information Warfare*, 181-2.

[11] USAF Fact Sheet 92-24.

[12] *Airman's Magazine*, Sept 94

[13] DARPA MEMS Vision, Internet address: http://esto.sysplan.com/ETO/FastPage.html, April 1995.

[14] IBM Information Technology Security Glossary, Internet address: http://www.ibm.com/security/glossary.htm, 13 December 1995.

[15] Corporate Anti-Virus Strategies Management Overview "Computer Viruses: Past Present, and Future," Symantec Corporation, Internet address: http://symantec.com/corpst.htm, 12 December 1995.

[16] *The First Information War*, 140.

Chapter 5

Planning the Information Warfare Campaign

Previous chapters provided a model to analyze systems employing information flows, thus identifying critical nodes and linkages. This model was then demonstrated in a concrete example—the Joint Force Air Component Commander. Next, tools and methods available to the information warrior were discussed. This chapter will draw these together, along with essential elements outside the scope of this paper, to provide a step-by-step approach to planning and executing an information warfare campaign.

Conducting information warfare, both to protect friendly systems and to attack hostile systems is, overall, very much like planning any other type of campaign. It requires that one know oneself for the former, and one's enemy for the latter. Armed with that knowledge, it also requires a clear understanding of the objectives that must be achieved. Once the system is understood and the objectives are clear, it requires one to select and employ the appropriate tool to accomplish the desired effect. Finally, it requires feedback to compare what was accomplished with the desired effects. In a nutshell, this is the four-step process for an information warfare campaign. Each of the steps will now be examined in greater detail.

Step 1: Analyze System

The first step in protecting a friendly information system or attacking an enemy system is to analyze the system. The goal of this assessment is to identify the individual elements, or nodes, of the system and the linkages between them. Although differing in purpose, and specific technologies and techniques, every system using information to obtain a particular end or ends will have certain functions it must accomplish. This is reflected in the Operational Architectures Model described in Chapter 2.

Using that model, one first assesses the functions of the system being analyzed. Next, one matches physical systems to the various functional areas which have been identified. This combination results in the Operational (Static) Architecture of the system, providing an understanding of the system at rest.

However, every system is dynamic. Thus, one must next look at the data and information architecture—the nature of data in the system and the protocols and methods for data transmission between functions. This is critical for the information warrior because it allows him or her to understand the element of time in the system, a particularly important element in the effort to get inside the enemy's decision-making loop. Once that has been accomplished, the planner has arrived at an understanding of the system in a dynamic state. By examining the dynamic model of the system, he or she can recognize critical nodes and linkages in the system with a view to targeting or protecting them, as appropriate. Armed with that understanding, the planner must now move to the next step, in which he or she determines what must be accomplished and which of the critical nodes and links, if affected, will bring progress towards the goals.

Step 2: Evaluate Objectives

Any type of warfare, information warfare not excluded, must be conducted to obtain political objectives. It is vital that the political objectives be clearly understood and that they be translated into coherent military objectives. As Clausewitz eloquently points out, "If we keep in mind that war springs from some political purpose, it is natural that the prime cause of its existence will remain the supreme consideration in conducting it.…The political object is the goal, war is the means of reaching it, and the means can never be considered in isolation from their purpose."[1] Obviously, objectives are situationally dependent, but the information warrior must make the trip from the political to the military to the informational objectives. This answers the basic question of why one is conducting information warfare—what one wants to accomplish. Answering this question allows the planner to determine the desired end state against which he or she can measure effects on the targeted system.

A clear understanding of the objectives and the desired end state permits the planner to move to the next phase of this step, the identification of the subject system's centers of gravity. Clausewitz defines these as, "the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[2] The key distinction between a critical node or linkage and a center of gravity lies in the relationship to the objectives. The goal of the information warrior is to identify those critical nodes and linkages in an enemy's information system which, if struck, would accomplish the objectives. Conversely, it is to identify the critical nodes and linkages in his or her own system which, if protected, would prevent an enemy from accomplishing

his objectives. These, then, are the system's centers of gravity. Once identified, one can move on to the next step in the process: selecting the appropriate tools to employ.

Step 3: Select Tools

The previous chapter described a few of the tools and methods available to the information warrior. In this step, he or she must select the appropriate tools based on several factors. First, of course, is availability. Obviously, not every tool in the information warfare arsenal will always be allocated for use at any level of warfare. Some will be reserved or will be allocated elsewhere for any number of reasons. In addition, many tools available at the strategic or operational levels of war will not be available at the tactical level. The information warrior must determine which tools are available for his or her use. If a tool is not available but is deemed critical, it must either be requested or a different selection must be made.

A second factor in tool selection is the effect the planner wants to achieve through targeting. According to the Air Force Target Intelligence Handbook, "The objective of targeting is to affect, change, modify, or impede enemy activity through destruction, damage, deception, or neutralization."[3] It is important to consider the full range of options and avoid the trap of only targeting for 100% destruction. This can result in wasting resources and unnecessary risk when mere neutralization might have sufficed. For example, as mentioned in the previous chapter, if an information collector such as a radar shuts down because of a computer virus or because the operator fears the potential presence of anti-radiation missiles, it is effectively neutralized without having to destroy it.

This example also serves to illustrate another element of determining what effect one wants to achieve, and that is duration. It may be desirable to affect elements of the system one is attacking for the long term, suggesting the selection of more destructive assets. Others, however, may simply need to be affected for short periods of time. In the above example, the shut-down of the enemy radar may serve to mask the entrance of an attack package at a certain time and place. In that event, a long-term effect is unnecessary and possibly a waste of resources. Different tools, used in different ways, can produce a variety of effects from destruction to neutralization, from long term to short. The information warrior must select and employ tools based on the right combination of effects which will allow him or her to obtain the objectives at minimum cost and risk.

The final factor in tool selection is assessing the target to determine its vulnerability to attack and attendant risks in attacking it. System elements identified as centers of gravity will often have been identified as such by an enemy as well. As a result, they will often be protected, reducing their vulnerability and raising the risk in attacking them. The planner must select tools which can feasibly thwart defenses and affect the target without undue risk. What is more, risk is not limited solely to the one applying the tool. It must be evaluated in a cost-benefit analysis at all levels. It must therefore be assessed in the larger context of overall objectives and a sense of balance must apply. For example, a planner may discover he or she has the means to destroy an opponent's banking system. The planner must assess whether or not the risk of economic suffering to the opponent's population and the international opprobrium this may earn the US are outweighed by the benefit of obtaining the objectives. It may well be that another, less drastic, method would achieve the objectives without such high costs.

It should be added here that, in information warfare, one is also planning for the protection of one's own centers of gravity. The planner must select appropriate tools to accomplish that mission, using many of the same basic considerations discussed above for the selection of tools for targeting an opponent's system. The primary difference lies in the objective.

Having developed an understanding of the system, determined the objectives, identified centers of gravity, and selected tools to apply, the information warrior then executes the mission. This brings the tool selection step to its culmination and moves the planner to the next step, assessing the results.

Step 4: Assess Effects

In the second step, the information warrior determined a desired end state for the system being attacked or protected. The third step led him or her to select specific effects which would bring about that end state and thereby obtain the objectives. In this step, one must compare actual effects with those desired, and must compare the overall impact on the system with the desired end state. This provides two feedback loops which will allow the planner to adjust efforts as necessary.

The first loop is the comparison of effects achieved in targeting or protecting individual elements with the desired effects established in Step 3. If surveillance reveals the effects were as desired, move on to other things. However, if the effects were not what were wanted, the planner must determine if the effect actually achieved (if any) is sufficient or if reattack is necessary. He or she must also evaluate why the effect differed from expectations to determine if the tool applied was inappropriate and/or the risk and

vulnerability assessment was defective. If reattack is required, the planner must take any necessary corrective actions, execute the reattack, and return to the assessment step as often as required.

The second assessment feedback loop involves the continuous comparison of the effects on the system as a whole with the desired end state established in Step 2. This provides the planner with a yardstick for measuring progress towards the campaign's objectives. It can tell one when to end the campaign and perhaps devote resources elsewhere. It can also clue the planner if centers of gravity were incorrectly assessed, allowing him or her to sharpen the model of the system and revise the selected centers of gravity, if necessary.

The four steps described above provide the information warrior with a method to plan and conduct information warfare. The planners of an information warfare campaign should be aware of some other considerations as well. These considerations relate to the role of technology, development, and culture. The first, in particular, is drawn from Lt Col Norman Hutcherson's discussion of them in relation to command and control warfare, but it is instructive for the larger subject of information warfare as well.[4]

Additional Considerations

The need for information is not asset dependent. Information warriors will face a variety of foes in various stages of technological development. Every one of them will require information to operate and a system to handle it no matter what level of technology is at their disposal. This means facing opponents whose information systems range from the sophisticated to the primitive and archaic. For example, during Operation

Restore Hope in Somalia, US forces tracked the warlord Aideed in Mogadishu using every technical capability at their disposal. The Somalian, on the other hand, used the drum to communicate. However primitive, he had an information system. Its primitive nature might have eliminated its vulnerability to the high-tech types of attack often associated with information warfare, but vulnerabilities to other attacks still existed. For the information warrior, analysis of the system must recognize these factors and he or she must be prepared to introduce weapons into the arsenal that are appropriate to the technology being faced. Do not fall into the trap of thinking something must be electronic to be information, a system, or worth attacking.

New technologies are increasingly available to anyone with money. They are developed and marketed by multinational corporations. This includes satellite imagery, portable global positioning system receivers, and encrypted and frequency-agile communications systems, to name but a few. Governments and other actors have become consumers of these technologies. Therefore, a third world country or non-state actor may well have access to the newest technology. The information warrior must not only avoid the trap of discounting primitive information systems, as discussed previously, but must also avoid the pitfall of assuming Third World foes will only have Third World information systems. Again, a careful system analysis is required without preconceived notions of what one will find.

Redundancy, or a lack thereof, is important to evaluate. As mentioned, some less-developed countries have access to the latest technology, but they may have little or no backup for those technologies in their information systems. Even highly developed foes who have neglected to invest in backups may lack redundancy. On the other hand, foes

who have multiple backups in their information systems may eliminate what would otherwise be critical vulnerabilities. The information warrior needs to carefully examine the enemy's depth of capability in identifying critical nodes and linkages.

The information warrior must avoid ethnocentricity. He or she must see the world through the enemy's eyes when attempting to structure an information warfare campaign. An understanding of the enemy's priorities, objectives, cultural biases and values is critical to anyone trying to analyze his systems and attack them or to protect his or her own from attack.

Conclusion

In this paper, the authors have attempted to provide a method for conducting information warfare. This was done in an effort to bridge an unavoidable gap between requirements and guidance. Requirements for planners to prepare information warfare campaigns are burgeoning as interest in this topic grows. On the other hand, doctrinal guidance remains embryonic. Even when published, information warfare doctrine must still be regarded as nascent since it lacks the major element upon which fully developed doctrine rests: experience which teaches us what tends to work. By employing the process described in this paper, the authors believe information warriors will be able to successfully conduct information warfare strategies in a variety of settings, ultimately leading to the development of a mature doctrine for information warfare.

Notes

[1] Clausewitz, *On War* (Howard & Paret, trans), 87.

Notes

[2] Ibid., 595-596.

[3] AFP 200-18, Vol I, *Target Intelligence Handbook: Unclassified Targeting Principles*, 1 Oct 1990, 5.

[4] Lt Col Norman B. Hutcherson, *Command & Control Warfare: Putting Another Tool In The War-fighter's Data Base*, Air University Press, Maxwell AFB, Sep 1994.

Bibliography

AFP 200-18, Vol I, *Target Intelligence Handbook: Unclassified Targeting Principles*, 1 October 1990.

Air Force Wright Laboratory, *Information Integration for Concurrent Engineering (IICE) IDEF3 Process Description Capture Method Report, AL-TR-1992-0057,* Wright Patterson AFB, Ohio, May 1992.

Air Force Wright Laboratory, *Integrated Computer-Aided Manufacturing (ICAM) Architecture Part II, Volume IV, TR-81-4023,* Wright Patterson AFB, Ohio, June 1981.

Air Force Wright Laboratory, I*ntegrated Computer-Aided Manufacturing (ICAM) Architecture Part II, Volume V, TR-81-4023,* Wright Patterson AFB, Ohio, June 1981.

Air Force Wright Laboratory, *Integrated Computer-Aided Manufacturing (ICAM) Architecture Part II, Volume VI-Dynamic Modeling Manual (IDEF2) TR-81-4023*, Wright Patterson AFB, Ohio, June 1981.

Air Intelligence Agency Briefing to Air Command and Staff College, 31 January 1996.

Airman's Magazine, September 1994.

Anson, Sir Peter, and Cummings, Dennis. "The First Space War: The Contributions of Satellites to the Gulf War," *The First Information War*, Campen, Alan D., ed., AFCEA International Press, Fairfax, VA, 1992.

Arquilla, John. *The Strategic Implications of Information Dominance,* Strategic Review, Summer 1994.

Computerworld, "Information Under Siege," 5 June 1995.

Computerworld, "New Laws Sought For Info Warfare," 5 June 1995.

Corporate Anti-Virus Strategies Management Overview, *Computer Viruses: Past Present, and Future,* Symantec Corporation, Internet address: http://symantec.com/ corpst.htm, downloaded 12 December 1995.

Daniel T. Kuehl, quoted by Gary H. Anthes in "*New Laws Sought For Info Warfare*," Computerworld, June 5 1995, v29, n23.

DARPA MEMS Program Vision Statement, Internet address: http://eto.sysplan.com/ ETO/MEMS/vision.html, downloaded 12 December 1995.

Deptartment of the Air Force Operational Concepts Primer for USAF Planning, DCS for Plans and Operations, USAF, 1 March 1995, 2.

Deptartment of the Air Force, *Cornerstones of Information Warfare*, 1995.

Deptula, Colonel David A. *Firing for Effect: Change in the Nature of Warfare.* Aerospace Education Foundation, August 1995.

Fadok, David S. *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, Air University Press, Maxwell AFB AL, Feburary 1995.

Hutcherson, Lt Col Norman B. *Command & Control Warfare: Putting Another Tool In The War-fighter's Data Base*, Air University Press, Maxwell AFB, September 1994.

IBM Information Technology Security Glossary, Internet address: http://www.ibm.com/security/FactSheets/glossary.htm, 13 December 1995.

Information Resources Management College of the National Defense University, *Information Warfare Definitions*, Internet address: http://vislab-www.nps.navy.mil/~sdjames/IW/Definition.html, as of 16 November 1993.

Information Resources Management College of the National Defense University, Internet address: http://vislab-www.nps.navy.mil/~sdjames/IW/Definition.html, as of 16 November 1993.

Joint Doctrine Capstone and Keystone Primer, 25 May 1995.

Libicki, Martin C. *What Is Information Warfare (Draft),* National Defense University, 21 July 1995.

Libicki, Martin C. *What Is Information Warfare,* May 1995, Internet address: http://ndu.edu/ndu/inss/strforum/forum28.html.

Magsig, Daniel E. *Information Warfare In The Information Age,* Internet address: http://www.seas.gwu.edu/infowar.html.

Mendel, William W. and Tooke, Lamar. "In The Systems Approach—A Primer" *Military Review*, Janurary 1993.

Report of the Defense Science Board Summer Study Task Force on Information Architecture For The Battlefield, Office of the Under Secretary of Defense For Acquisition & Technology, Wash DC, October 1994.

Report of the Defense Science Board Summer Study Task Force on Information Architecture For The Battlefield, Office of the Under Secretary of Defense For Acquisition & Technology, Wash DC, October 1994.

Schwartau, Winn. *Information Warfare*, Thunder's Mouth Press, NY, 1994.

Sun Tzu, *The Art of War*, translated by Samuel B. Griffith, Oxford University Press, 1963.

The Economist. *The Ties That Bind*, 10 June 1995.

Toffler, Alvin and Heidi. *War And Anti-War*, Warner Books Inc., NY, 1993.

Toma, Joseph S. "Desert Storm Communications," *The First Information War*, Campen, Alan D., ed., AFCEA International Press, Fairfax, VA, 1992.

Toma, Joseph S., "Desert Storm Communications," *The First Information War*, Alan D. Campen, editor, AFCEA International Press, Fairfax, VA, 1992.

United States Air Force Fact Sheet 92-24.

United States Air Force Fact Sheet 92-63.

US News & World Report. *The Gulf War Flu* , 20 Janurary 1992.

Von Clausewitz, Carl. *On War*, Howard & Paret, translation, Princeton University Press, Princeton, NJ, 1989.

War Theory Coursebook, "Air Campaign Planning," Air University Press, Maxwell AFB, AL, 1995.

Warden, J.A.. "The Enemy as a System." *ACSC Strategic Structures Coursebook* Volume II, FY95.