

AU/ACSC/068/2000-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

“OPERATIONALIZING”
INFORMATION OPERATIONS

by

John R. Glock, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Carol Atkinson

Maxwell Air Force Base, Alabama

April 2000

Distribution A: Approved for public release; distribution is unlimited

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

	<i>Page</i>
DISCLAIMER	ii
LIST OF ILLUSTRATIONS	v
LIST OF TABLES	vi
PREFACE.....	vii
ABSTRACT.....	viii
INTRODUCTION	1
Offensive Counterinformation.....	2
BACKGROUND	4
Basic Concepts	4
Joint Targeting Process.....	6
Commander’s Objectives and Guidance	7
Target Development	8
Weaponneering Assessment.....	8
Force Application	9
Execution Planning/Force Execution	9
Combat Assessment.....	9
Offensive Counterinformation.....	10
Target Types	10
Offensive Counterinformation Functions	11
OCI “Targeting” Process	12
ISSUE ANALYSIS.....	14
IO Targeting Concepts.....	14
Objectives and Guidance	19
Target Development	20
Implications of IO/IW on Target Development.....	20
Weaponneering	25
Force Application	26
Execution	27
Combat Assessment.....	27
CONCLUSIONS AND RECOMMENDATIONS	32

Conclusions	32
Systematic Approach Required	32
Joint Targeting Process.....	33
Offensive Counterinformation Targeting Process	33
Recommendations	33
Develop IO Target Materials.....	34
Develop IO Critical Elements for Generic Installations.....	34
Develop IO Target Folders Requirements.....	35
Develop Joint IO Weaponneering Methodologies	35
Fully Integrate Information Operations with Other Operations	35
Ensure Adequate Access	36
Refine IO Terminology.....	36
Summary.....	36
ANNOTATED BIBLIOGRAPHY	37

List of Illustrations

	<i>Page</i>
Figure 1. Joint Targeting Cycle	7
Figure 2. Information Targets Types	10
Figure 3. Levels of Offensive Counterinformation Operations	11
Figure 4. Generic System Model	15
Figure 5. Information Flows	17

List of Tables

	<i>Page</i>
Table 1. Components of Offensive Counterinformation	2
Table 2. Recommendations.....	34

Preface

Many people have already written about information operations (IO), information warfare (IW) and information in warfare. Therefore, you may well ask why should I read yet another paper on the latest craze to seize the U.S. military and the myriad of academicians and contractors that write about the military. This is a fair question. I intend to offer you something different from what I – and what I believe you -- have previously read. Most of the material available on this subject addresses the theory and potential of information operations in the future. I believe the future is here! What I have done in this paper is analyze a process by which one can actually move information operations from the world of arcane theory to operational employment.

I would like to acknowledge the tremendous assistance rendered by Major Carol Atkinson, my research advisor. Without her help and guidance, this paper would not have been possible. I would also like to thank Mr. Arnold Abraham and Mr. Jay Hagler of the Defense Intelligence Agency, Mr. Greg Raddabaugh of the Joint Information Warfare Center and Lt. William Garrity of the Naval Information Warfare Activity. Their assistance in writing this paper was invaluable. Without their inputs and guidance, I could not have written this paper.

Abstract

All military operations utilize information operations (IO). The Joint Staff and Services have written doctrine on IO. The cornerstone documents of the Joint Staff and Services, all refer to IO. Information Superiority is a core competency of the United States Air Force. Yet, there is virtually nothing written on how one actually operationally employs IO in support of a Joint Force Commander. The purpose of this paper is to address the question: “How, at the operational level, does one employ offensive counter information operations (OCIO)?”

This researcher decomposed the problem of employing OCIO into constituent parts. This methodology revealed that successful employment of OCIO requires a force application process similar to that used when employing traditional forms of military force (e.g. air power). One still needs to establish objectives, identify targets, recommend capabilities, apply these capabilities against specific targets and after applying them assess their level of success. Having established the requirements of a process for employing OCIO, this paper then analyzes what aspects of the current joint targeting process need modification, and how to modify them in order to apply that process to OCIO.

OCIO can use the existing joint targeting process with only minor modifications. To enhance the OCIO targeting process there are seven recommendations. These are: creating IO Target Materials, developing IO critical elements, establishing IO target folders requirements, formulating joint IO weaponeering methodologies, integrating IO and non-IO planning efforts, ensuring adequate access to IO capabilities and refining terminology.

Part 1

Introduction

Military information functions are essential to our combat operations – they are a tool for achieving the Joint Force Commander’s campaign objectives. Targeting the enemy’s information functions keeps him from achieving his.

— Cornerstone of Information Warfare

All military operations utilize information operations. The Joint Staff and Services have all written doctrine on information operations. The cornerstone documents of the Joint Staff and Services, all refer to information operations. The United States Air Force identifies Information Superiority as core competency.¹ Yet, there is virtually nothing written on how one actually operationally employs information operations in support of a Joint Force Commander.² The purpose of this paper is to address the question: “How does one employ information operations?”

This paper is about employing offensive counterinformation operations (OCIO) in support of a Joint Force Commander (JFC). The focus is on OCIO at the operational level of war. CI “is an aerospace function that establishes information superiority by neutralizing or influencing adversary information activities to varying degrees . . .”³ More specifically, it concentrates on Offensive Counterinformation (OCI) operations. OCI is “offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting and deceiving the adversary’s information and information systems.”⁴ Several air power theorists have stated that air power is targeting.⁵ The same is true of OCIO. This paper examines a process for OCIO targeting.

Operations in the information domain open a new range of targeting possibilities complementary to those traditionally explored in the effective employment of kinetic weapons. To take advantage of these new opportunities for engaging an adversary, planners need not invent a new process. The task facing military planners remains the same; the execution is different. Successful OCIO requires a systematic approach to establish objectives, translate them into actionable entities (targets), determine what capabilities can achieve the desired results and after execution assess the level of success one has achieved. It needs emphasizing that this is true for all the components of OCIO (See Table 1)⁶.

Table 1. Components of Offensive Counterinformation

Offensive Counterinformation
Psychological Operations (PSYOP)
Electronic Warfare
Military Deception
Physical Attack
Information Attack

Source: Department of the Air Force, *Air Force Doctrine Document 2-5, Information Operations* (Washington D.C., August 1998), 3.

Starting from the premise that Offensive Counterinformation Operations require a systematic process, Part 2 of this paper provides needed background information on OCIO targeting. First, there is a discussion of basic concepts. Following this is a brief description of the current joint targeting process. Next is a broad overview of what OCIO are.

With the knowledge of the joint targeting process and OCIO, in Part 3 the reader looks at the relationships between the traditional targeting process, and the process that is required to successfully engage in OCIO. In this section, the reader will see how the joint targeting process applies to OCIO, as well as what modification are needed to make this process fully applicable to OCIO.

The joint targeting process is applicable to OCIO. In doing the research for this project, several issues arose that must be addressed to meet fully the goal of applying the joint targeting process to OCIO. These issues are: creating IO Target Materials, developing IO critical elements, establishing IO target folders requirements, formulating joint IO weaponeering methodologies, integrating IO and non-IO planning efforts, ensuring adequate access to IO capabilities and refining terminology.

Notes

¹ Department of the Air Force, *Air Force Doctrine Document 1, Air Force Basic Doctrine*. (Washington D.C., Sep 1997), 31-32.

² Both Joint Pub 3-13 and AFDD 2-5 address targeting, but neither goes beyond the most superficial discussion of the subject. Joint Pub 3-13, p II-13 provides little more guidance than: “offensive IO targeting . . . should consider all elements of the adversary’s national power to determine how best to achieve desired objectives.” AFDD 2-5, p 34 does little better, “The IW team evaluates information target systems, functional relationships, and friendly and adversary critical nodes and recommends appropriate offensive and defensive IW missions for inclusions in the ATO.”

³ Department of the Air Force, *Air Force Doctrine Document 2-5, Information Operations*. (Washington D.C., 1998), 9.

⁴ *Ibid.*, 42

⁵ Col Phillip S. Meilinger, *10 Propositions Regarding Airpower*, (Air Force History and Museum Program, 1995), 20.

⁶ There are objectives for both PSYOP and deception. There are different targets each these components can attack. PSYOP or deception planners may want to target a senior decision-maker, the general population or a component of enemy fielded forces. In addition, planners can use different means (e.g. leaflets, broadcast, drones, demonstrations, etc.). There is a need to determine which combination of targets and means will likely achieve the desired result. Finally, there will be observable indications of the success of these operations (e.g. Iraqi forces left in place to defend against an amphibious operation).

Part 2

Background

Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past, and is seen as an indispensable and synergistic component of air and space power.

— AFDD-1

Basic Concepts

Throughout history, gathering, exploiting and protecting information has been critical to policy makers. The unqualified importance of information will not change in the 21st century. What has changed is the increased vulnerability of information and information systems, as emerging opportunities are developed to exploit the information domain. Sustaining the responsive, high quality data processing, information and decision making processes needed for joint military operations will require more than just an edge over an adversary. We must have information superiority¹: “The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or deny an adversary’s ability to do the same.”²

Information superiority is essential to attaining dominant manoeuvre, precision engagement, full dimensional protection and focused logistics.³ Information superiority is achieved by means of information operations. DoD defines Information Operations as actions taken to affect adversary information systems while defending one’s own information and information systems⁴. The concept of offensive counterinformation operations (OCIO) is consistent with the

tenets of modern warfare in which shattering an adversary's overall cohesion and will to fight is paramount. It calls for an attitude of mind in which doing the unexpected; using initiative and seeking originality are combined with a ruthless determination to succeed. It applies across the full spectrum of military operations from peace through crisis, conflict, and back to peace. In essence, information operations are actions taken to influence decision-makers⁵, and this will require a new approach to targeting, but not necessarily a new targeting process.

Operations in the information domain open up a new range of targeting possibilities, which are complementary to those traditionally explored in the effective employment of kinetic weapons. In the future, targeteers must look at the battlespace with a holistic approach, when conducting targets systems analysis and target development, and take into account potential vulnerabilities presented by cultural, psychological, virtual and "information process" factors. For example, target system analysis must include an examination of the decision-making process, ranging from human factors through information flows to critical facilities or virtual nodes, to the media which an adversary might use to influence or suppress public opinion, both within his own territory and externally. Accordingly, the target list of the future might include information systems, key individuals, the need to change the perception of the adversary's population, as well as the traditional critical elements of key systems and processes. This will require adaptation of the mindset in the targeting and operational planning communities.

Targeting in the information domain has the same requirements as does targeting for conventional kinetic weapons. However, OCIO targeting requires a much wider range of intelligence and analytical expertise. Intelligence requirements will need to be developed and resources allocated, since the fidelity and level of detail required are of a much greater magnitude than previously needed. Today planners need to know more than the function of a

target. They may need to know the type operating system, make of firewall and patches used for a specific computer server, or detailed biographical data on a decision-maker. This will require targeteers to state clearly the aim for which the analysis is being conducted, determine intelligence gaps, and provide tasking to the relevant agencies or sources. Similarly, the need for effective combat assessment (CA) in the information era will require analysts to develop battle damage indicators and change detection methodologies to replace electro-optical imagery of physical damage from conventional munitions. At the time targets are being selected, it is also essential that commanders and decision-makers be apprised of the potential collateral damage⁶ implications of various OCIO capabilities. In this respect, target clearance procedures should follow those currently used for conventional weapons i.e. legal⁷, proportional, intelligence gain-loss and collateral damage estimates. OCIO targeting will generate many new requirements.

There is so much new in the arena of information operations that we forget the traditional processes can still apply to evolving capabilities. OCIO targeting still requires translating the commander's intent and desired end-state into actionable objectives (objective determination). One must still select those activities one desires to affect (target development), and estimate the probability of achieving a desired result (weaponing). Finally, after execution the actual results will need to be assessed (combat assessment). While the joint targeting process and OCIO targeting process has the same broad requirements, the difference in execution requires new or modified data, formats, products and methods.

Joint Targeting Process

Targeting is the process of selecting those entities against which military action should be directed to achieve the desired results, and matching the appropriate response to them taking into account operational requirements and capabilities. The appropriate responses include both lethal

and non-lethal capabilities. The primary responsibility for joint targeting resides with the JFC. The joint targeting cycle (Figure 1. Joint Targeting Cycle) is a conceptual model used to describe the process of selecting targets for attack, which have the greatest likelihood of accomplishing the JFC's war fighting objectives. The cycle provides a logical progression for determining targeting solutions. It proceeds from the definition of the problem to an assessment of the solution for that problem. The steps are iterative and omni-directional. This cycle is a continuous process, which consists of six phases: objective determination, target development, weaponeering, force application, execution planning/force execution and combat assessment. ⁸

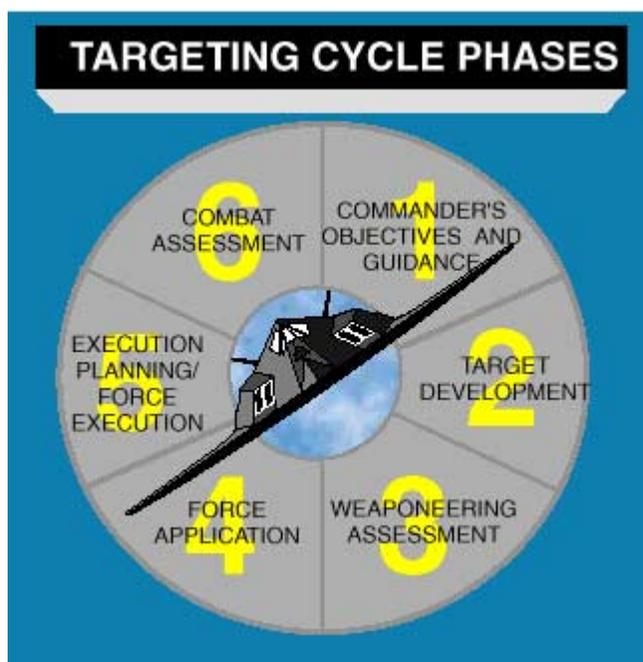


Figure 1. Joint Targeting Cycle⁹

Commander's Objectives and Guidance

The development of objectives and guidance is the first and most critical step in the targeting cycle. Objectives drive the entire targeting process. An objective defines the desired end state. Guidance provides the framework for achieving the objective. Together they identify what is to be achieved and under what conditions and parameters. Without clear understanding

of what JFC wants to achieve, it is impossible to devise efficient targeting strategy. The value of target selection and analysis depends on a clear understanding of objectives and guidance.¹⁰

Target Development

Target development is the systemic examination of potential target systems, their components and the elements that make up each component in order to determine the importance, attack priority and weight of effort for specific target systems. The sole purpose of target development is to translate the commander's objectives and guidance into a list of targets. Efficient application of force is the underlying goal. The process by which one achieves that efficiency is open-ended analysis to determine which targets will likely satisfy the objectives, and the specific nature, extent and duration of damage one needs to inflict on those targets. The output of target development is a prioritized list of installations, forces and activities that if attacked will have the greatest likelihood of accomplishing the commander's objective.¹¹

Weaponeering Assessment

Weaponeering is the process of determining the quantity of a specific type of lethal or non-lethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapon effects, munitions delivery accuracy, damage criteria, and weapon reliability. Essentially, it is the process of finding the proper weapon to accomplish a given objective with the minimum force required. Weaponeering solutions give an estimate of the expected performance of a nominal weapon in an infinite number of identical trials. They do not predict the results of any specific weapon. Instead, they provide a probabilistic estimate of the expected results¹²

Force Application

Force application is the process by which a staff provides the commander with fused weapon system recommendations against a target system and its vulnerabilities. During the force application process, recommendations are made on how to apply available forces and weapons effectively and economically in order to achieve the JFC's desired objectives. In this step planners optimize the available resources with the prioritized targets in order achieve the wanted effects ¹³

Execution Planning/Force Execution

Execution planning begins after the JFC approves the force execution recommendations and includes actions taken in preparation for attack once the commander approves the force applications recommendations. During execution planning targeteers provide the target intelligence portion of tasking orders; supply tasked combat units with target intelligence, target materials, and other mapping, charting and geodesy (MC&G) products; and assist with the preparation for the combat assessment.¹⁴

Combat Assessment

The final phase in the targeting cycle is combat assessment (CA). This phase is divided into four functions: battle damage assessments (BDA), munitions effect assessments (MEA), reattack recommendations (RR) and mission assessment (MA). BDA is the timely and accurate estimate of effect on a target and target system resulting from the application of military force, either lethal or non-lethal. The MEA seeks to identify, through a systematic trend analysis, deficiencies in weapons system and munitions performance or combat tactics. The RR flows directly from both BDA and MEA efforts. It assesses whether an objective has been achieved,

and whether or not a change in tactics is required. In MA, analysts assess if a component (e.g. the air component) has accomplished an assigned mission such as air superiority¹⁵

Offensive Counterinformation

Target Types

Offensive counterinformation operations target information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems (Figure 2. Information Operations Targets Types). At the strategic level, OCIO seeks to influence adversary decisions in favor of US interests¹⁶ (Figure 3. Levels of Offensive Counterinformation). At operational levels, the target is the information-dependent process; whether human or automated that affects the employment of forces. While at the tactical level OCIO looks at affecting the ability to engage friendly forces

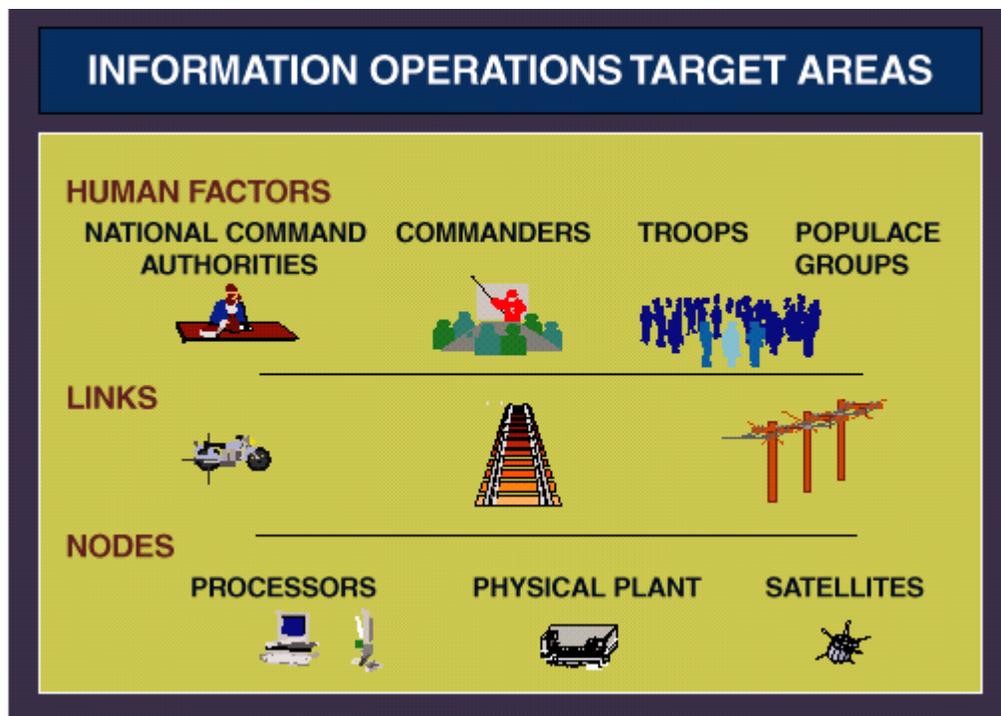


Figure 2. Information Targets Types¹⁷



Figure 3. Levels of Offensive Counterinformation Operations¹⁸

Offensive Counterinformation Functions

Offensive counterinformation operations consist of five primary components or functions. These are psychological operations, military deception, electronic warfare (EW), physical attack and information attack. OCIO require a thorough understanding of an adversary’s information use and information systems, to include capabilities, dependencies and vulnerabilities¹⁹. These components can be applied as part of an over-arching IO strategy. For example, physical attacks on telephone switches to isolate the NCA could be used in conjunction with deception operation intended to persuade the NCA that there is an ongoing coup. OCIO is also a means to achieve objectives as part of an operational campaign or tactical or engagement. For example, an asset

could generate electromagnetic pulses as part of an EW attack in order to burn out circuits of an aircraft, causing it to crash - a tactical engagement, which directly degraded combat power of an opposing military force.

OCI “Targeting” Process

Regardless of the types of targets, level of operations, or OCI component utilized, one must apply some systematic process in order to successfully employ counterinformation capabilities. As with existing capabilities, one needs to establish objectives, identify targets, recommend capabilities, apply these capabilities and assess the level of success of the application of these capabilities. It is evident from the previous discussion that successful employment of information operations requires planners either to use the current joint targeting process (appropriately modified), or to create an analogous (and possibly redundant) process.

Notes

¹ Joint Chiefs of Staff, *Joint Vision 2010* (Washington D.C., undated), 16.

² Department of the Air Force, *Air Force Doctrine Document 2-5, Information Operations* (Washington D.C., 1998), 41.

³ Ibid.

⁴ Department of Defense, *Joint Pub 3-13, Information Operations* (Washington D.C., 1994), II-14.

⁵ Decision-makers exist at all levels of conflict not just at the NCA or JFC level. For example, the decision not to engage an ingressing aircraft or to engage a drone could be a decision of a surface-to-air missile battery commander. In addition, a decision-maker need not be a human. An automated control process such as a supervisory control and data acquisition (SCADA) system may make a decision about load curtailment for an electric power network.

⁶ A review of current literature finds little reference to collateral damage. However, this is a real problem. For example, many people talk about using viruses to attack an adversary’s information systems. If a particular piece malicious code replicates itself and infects any system it contacts, one can conceive of a scenario where this code could infect a hospital’s computers causing untold damage with the potential for loss of civilian life.

⁷ Aspects of OCIO will add additional legal considerations beyond those associated with the Law of Armed Conflict. For example, International Telecommunications Law needs to be considered. The 1982 Nairobi Convention prohibits harmful interference with telecommunications.

Notes

⁸ Department of the Air Force, *AFP 14-210, USAF Intelligence Targeting Guide*, (Washington D.C., 1998), 8.

⁹ Department of Defense, *Joint Pub 3-56.1, Command and Control of Joint Air Operations*, (Washington D.C., 1994), IV-1.

¹⁰ Op. cit. 9

¹¹ Ibid.

¹² Ibid.

¹³ Ibid., 10

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Department of Defense, *Joint Pub 3-13, Information Operations* (Washington D.C., 1994), II-14.

¹⁷ Ibid.

¹⁸ Ibid., II-2.

¹⁹ Department of the Air Force, *AFDD 2-5, Information Operations*, (Washington D.C., 1998), 10

Part 3

Issue Analysis

We are committed to maintaining information superiority – the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary’s ability to do the same.

— A National Security Strategy for a New Century, 1999

IO Targeting Concepts

To meet the challenge levied on us by the President, we must find the means to employ offensive counterinformation successfully. Planning for physical destruction of targets is a core competency of traditional targeting. Offensive counterinformation operations (OCIO) represents a new function which targeteers must be prepared to support and make a core competency. This paper has discussed the joint targeting process and the concept of OCIO. It now looks at integrating these concepts. Targeting involves the systematic examination of an opponent in order to select targets and match the appropriate response to them taking into account operational requirements and capabilities. The process should not be started with either a target or a weapon already chosen. Rather one must start with an understanding of the desired end state. This, combined with a thorough understanding of the opponent allows planners to determine suitable military objectives. These military objectives are really the activities one wants to affect in order to achieve the desired end state. These activities in turn are accomplished or supported by

various systems. From these systems, targeteers derive targets and the elements at those targets against which to apply a specific capability.

It is essential to understand the concept of a system. All systems consist of certain generic components (Figure 4. Generic System Model). An information system can be defined as a group of interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization. Information systems can be manual and rely on paper and pencil, or they can be computer based and rely on computer hardware and software to process and disseminate information. It is important to remember that even in a computer based information system; computers are only part of the information system. To understand an information system, one must understand the problems it was designed to solve, its architectural and design elements, and the organizational process. One must also be familiar with the environment in which the system exists.

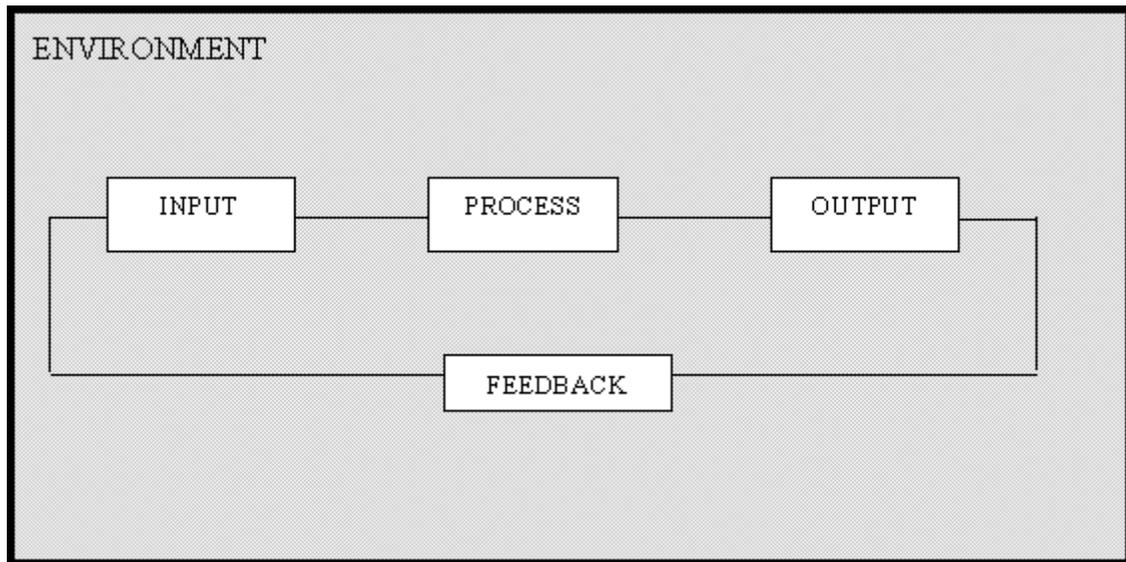


Figure 4. Generic System Model

The above model can be applied with equal ease to human or computer based information systems. It could represent a national leader's decision making process. "Inputs" consist of many things (e.g. press reports, intelligence and advice from trusted advisors). The "Process" consists of the decision-making procedure a leader uses. Outputs may also consist of many components (e.g. presidential directives and press releases). On the other hand, it could be a Supervisory Control and Data Acquisition (SCADA) system for an electric power grid. Inputs would include information on load, status of equipment; etc. reported by remote terminal units (RTUs) located throughout the grid. Processes include various energy management functions. Outputs consist of various directions issued to the RTUs about such things as load shifting.

What is important is that attacking any component can influence the entire system. Planners can plan to attack the inputs to the process, the process itself, the outputs, feedback or environment. Using the commander's objectives, targeteers can determine the optimum point for the attack. His objectives should tell us when he wants the effect felt, for how long, to what degree, and any restrictions, such as no long-term damage. The best way to attack or influence a target system may be by means of information operations.

When considering attacks on an information system, it is easiest to view information as flowing from a source to a destination. Figure 5a depicts this flow. The additional figures (5b-d) show the four general categories of information flow.

Interruption occurs when an asset of the system is destroyed, becomes unavailable or unusable, or is overpowered. This is an attack on availability. Examples include destruction of a piece of hardware (e.g. hard disk), cutting a communication line, disabling a file management system, jamming a signal. Interruption is essentially a denial of service type of attack. It can

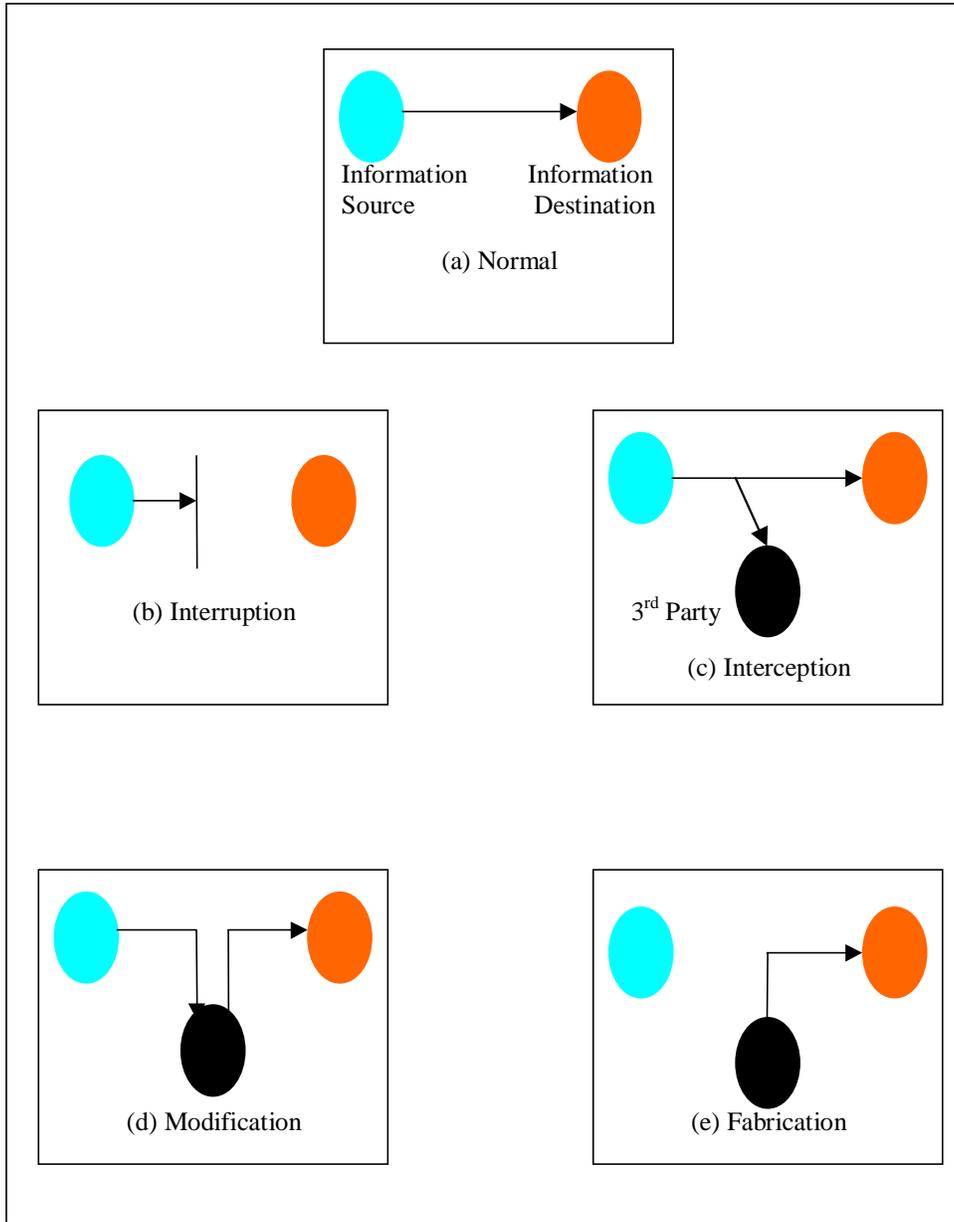


Figure 5. Information Flows¹

range from attacking an information node in an information system with conventional resources such as TLAMs attacking a switch in a telecommunications system, to jamming a microwave relay link. It also includes such things as attacking a computer based information system with a WORM that effectively consumes the resources of a system.²

Interception is the unauthorized access to an asset. This is an attack on confidentiality. Examples include wiretapping to capture data on a network, illicit copying of a file or program, and RF intercept. OCI operators can conduct interception in order to release confidential information about an adversary to unauthorized parties (e.g. the media). In addition, analyst can use interception for the purpose of traffic analysis. This information can help one determine the location and identity of essential sources and destinations in an information system. This information can be extremely useful in prioritizing nodes for attack. Methods range from traditional forms of SIGINT to such activities as packet sniffing.³

Modification is unauthorized tampering with the information in an information system. This is an attack on data integrity. Examples include changing the values in a data file, altering a program so that performs differently, and modifying the contents of a message. Modification of information includes such things as morphing a television broadcast from a leader and re-broadcasting the new message, to changing access on accounts to gain wider access to the system and altering the coordinates in an installation database. Modification can also include inserting data bits or grams to create an error-checking problem. This form of modification is actually a form of interruption.⁴

Fabrication is the unauthorized insertion of counterfeit information. This is an attack on authenticity. Examples include the insertion of spurious messages or the addition of records to a file. Activities range from traditional forms of propaganda to creation of false data in a database.

Another example is military deception. A well-known example of deception was the use of Gen. Patton and a fabricated army built around him to deceive the Germans as to the location of the D-Day landings in World War II.⁵

Understanding how systems function and the various opportunities to influence it provides the foundation for participating in the first step of the joint targeting process – objective determination. Knowing the ways of attacking the flow of information within a system provides targeteers with the tools to apply the joint targeting process to OCIO.

Objectives and Guidance

Combatant commander's staffs produce strategic estimates. These result in operational concepts and courses of action. One of the critical parts of this estimate process is defining the strategic end state to be achieved. The key to an integrated approach between targeting and IO begins with the interpretation of the Commander's intent, objectives and guidance. The commander's staff must consider IO options early in the commander's decision making process. This requires close coordination between the targeting staff and IO staff. Targeting staff officers should be an integral part of the IO Cell. These officers should be familiar with IO concepts and techniques as well as standard targeting practices.

In modern conflict, one can support almost any objective through OCI techniques. For example, degrading an adversary's air defense posture could be achieved through attacking the underlying automated processing network of the IADS with malicious code rather than physically destroying the radars and missiles. With this principal in mind, the IO Cell and Targeting Cell should jointly review all objectives.

Objectives must be attainable, quantifiable and unambiguous. Objectives can normally be achieved by various methods such as physical attack, information attack or deception. Which of

these methods is best will be determined by means of the rest of the targeting process. Objectives drive the entire targeting process allowing planners to find the optimum mix of targets and offensive capabilities given the operational constraints and restraints at the time.

Target Development

Target development flows from the JFC's objectives and guidance. The sole purpose of target development is to translate objectives and guidance into lists of appropriate targets. As stated earlier, target development is the systematic examination and evaluation of potential target systems, their components and the elements that make up each component to determine those against which military action can be directed to achieve given objectives.

The first function in target development is to identify target systems that support the enemy activity to be affected. The target system concept is important because almost all targeting is based on targeting systems, not individual targets. A single target is rarely significant because of its own characteristics. Its importance more often lies in its relationship to other components within the system it belongs. It is critical to understand the concept of a system, be it a POL, WMD or information system. One of the keys to successful target development is understanding the relationships between, within target systems in order to uncover vulnerabilities, and identify critical elements for targeting. This is most relevant to OCIO or targeting information systems that support other systems. Targeteers must include the impact of an adversary's reliance on information in investigating these relationships.

Implications of IO/IW on Target Development

The fundamentals of target development have not changed as a result of the addition of IO/IW target sets and operations. The traditional target development methodology of identifying target system components, elements and critical elements is still valid. What has changed, is the

scope of the intelligence preparation of the battlespace (IPB) effort, an expansion of the components and elements to be examined, and correspondingly an increase in the intensity of the collection/production effort required.

Target system analysis (TSA) must be conducted in manner that recognizes the synergistic relationship between human nature, topography, communication architecture, time, information flow and traditional target functionality. Targeteers must seek to include these inter-related elements when analyzing processes/systems in order to identify their critical elements. In addition, it is important to realize that expanding the scope of the TSA will increase the probability of identifying critical elements that analysts may not have considered using traditional target development methodologies. Also, it may be possible to identifying a series of elements which if targeted individually would not achieve the desired objective but targeted together have a synergistic, objective achieving effect.

As mentioned earlier, the target development effort should use a synergistic approach when evaluating a targeted system/process. Developing a framework to organize and systematically evaluate the components and elements of a target system is vital. In the information age, all aspects of information flow must be examined in order to expose interrelationships and criticality. Analyzing organizational relationships (*Hierarchical Domain*), component and element functions (*Functional Domain*), the actual flow of information (*Logical Domain*), the type and structure of information being passed (*Informational Domain*), and the physical architecture utilized to pass the information (*Spatial Domain*) may lend insight into the synergistic nature of the process.⁶

The following template of domains provides a framework for conducting both IPB and TSA. To illustrate, an integrated air defense system (IADS) will be used as an example of a

system/process under review. The objective for this example is to prevent air interceptor operations from a specific airfield for a period of X hours.

Hierarchical Domain: Is the description of the leadership architecture within any group, organization or process. For example, a description of the hierarchical domain of the IADS would detail the relative ranking of the components and elements of the process. The components and elements would include leaders (Sector Operations Center (SOC) commander, squadron leaders), commands (SOC, Ground Control Intercept (GCI) sites), and organizations involved in the IADS. Examples of critical elements derived via an examination of the hierarchical domain might include the local SOC commander, GCI controller, etc.⁷

Functional Domain: Is the description of the role of each element within the hierarchical domain. For example, in the IADS example, the functional domain description would explain the roles played by GCI sites, SOCs, SAM sites, interceptors, etc. Examples of critical elements of the functional domain may include the GCI sites, fighter aircraft or airfields.⁸

Logical Domain: Is the description of the actual flow of information within the targeted process. The description ignores components and elements listed in the hierarchical domain which serve no function of concern given your objective. For example, SAM site may be listed in the hierarchical or functional domain but is not incorporated into the logical domain representation because it has no bearing on your objective of preventing fighter activity from a specific airfield.⁹

Spatial Domain: Is the description of the physical architecture over which information is flowing. This description would include telecommunications architecture, links, nodes, bridges, etc. Examples of critical elements derived via an examination of the spatial domain may include fiber communication lines at bridge crossings (destroy the bridge, destroy the link), satellite

downlink sites, troposcatter sites, landline junctions, etc. In the IADS example, scramble orders passed to an airfield over landline might be the critical vulnerability and the spatial description might identify a landline junction as the critical element.¹⁰

Informational Domain: Is the description of the information being passed through a targeted process to include the medium and structure. For example, unencrypted voice communication passed using VHF radio to airborne fighter aircraft. Another example would be air surveillance track information passed via an encrypted signal by radio microwave systems. Examples of critical elements derived from an examination of the informational domain may include the targeted signal itself or some unique feature of the way it is transmitted. In the IADS example, the voice GCI communications could be the critical element.¹¹

Temporal Domain: Is the description of the amount of time a system requires to pass information within a targeted process. An example of critical elements within the temporal domain may include an essential telecommunications processing facility. In the IADS example, timeliness of the scramble order or of GCI commands may be a critical element.¹²

The key to using the six domain methodology in target development is to realize that cultural factors, synergistic effects (such as targeting multiple non-critical element to produce a critical effect) and the commanders intent must all be weighed carefully in the process of identifying critical elements. One of the possible critical elements identified as a result of target development may be an information processing system such as a personal computer, processing node, switching center, etc. It is important to recognize at the time of target development; weaponeering options are not considered, however, conducting IPB in today's information driven environment demands expansion of the scope of the effort.

Offensive counterinformation operations require targeteers to evaluate all the domains outlined above but with increased emphasis on the informational and functional domains. Once the functionality of a component or elements has been identified, obtaining the details of the information processing architecture within the node is critical. For example, targeteers can recommend attacking an electric power grid through the remote maintenance network to disrupt the SCADA controls. Information on the software and hardware configuration of the network would be an essential part of target development for such an operation. These "cyber" aspects must be considered in developing the criticality and vulnerability assessments for target system components and component elements.

Historically, vulnerability assessment has been oriented towards the type of weapons available – i.e. kinetic. Concepts such as Depth, Cushion and Reserve¹³ are not fundamentally changed by addition of IO capabilities. On the other hand concepts such as Dispersion and Physical Characteristics must be take on a broader meaning in order to be useful measures of vulnerability in regards to IO. Geographic separation of target elements may be irrelevant in cyberspace.

Dispersion and Physical Characteristics do have corollaries that one can apply in OCI analysis. First, when targeting a system through its automated information network, one must assess the heterogeneity of the network. Are all of the computer systems and operating software the same, or are there multiple variations on the network? How will these different components react to the particular capability being considered for use? A “dispersed” network would have a greater degree of heterogeneity, and thus more resistance to information attack. Another part of this assessment would be to determine if the network is inter-connected or stand-alone.

Physical characteristics traditionally looked at mobility in order to take into account the problem of perishability of information along with our ability to detect, locate and identify a target component. Although physical mobility is not an important issue for a possible computer network attack (CNA) weapon application, the problems of perishability and ability to access a target remain valid. In fact, these factors have the greatest influence in conducting CNA since the cyberspace environment is far more fluid than its physical counterpart. Countermeasures are also considered as part of this assessment. Instead of looking at terrain and camouflage, targeteers must assess internal network configurations such as firewalls and other access controls.

Target development and identification of critical elements is dependent upon the quality of the information provided to the analyst. To support the six-domain method of analyzing a targeted process, collection and production requirements must be proactively developed and processed. Once target development is complete, planners can match resources with the targets

Weaponneering

Decision-makers need a method that will provide them with an idea of the probability of success when using any capability, as well as a means of determining the cost in resources. Historically, quantitative methods are used to measure the extent of damage rendered by kinetic weapons. Physical damage is analyzed and translated into functional damage. These methods are based primarily on Joint Technical Coordinating Group for Munitions Effects (JTCEG-ME) publications, which define effectiveness indices, based on blast, fragmentation and fire effects of weapons and fires. No one has conducted this level of analysis for information operations capabilities. Yet, this is a requirement for scientific calculations of the effect of force application. Non-kinetic weapons will still produce some type of discernible change. For

example, shutting down a plant will change its infrared signature. Thus, traditional analysis methods will provide functional damage estimates.

However, targeteers require a joint standard for OCI capabilities. Joint IO weaponizing methodologies need to be developed. This will allow targeteers to produce probabilistic estimates of the likelihood of success for a given attack. It will also provide commanders and planners with a method for comparing the relative degree and likelihood of success, as well as the relative cost of each capability planned.

There is a need for the equivalent, of a Joint Munitions Effectiveness Manual for differing types of IO capabilities. These manuals will need to provide detailed data on the capabilities and target interaction similar to existing effectiveness indices. In addition, one needs target vulnerability data that includes different damage criterion. Finally, a methodology for assessing and computing the probable outcome of using a specific capability against a specific target is needed.

Force Application

Effective force application requires in-depth knowledge of available OCI weapons along with conventional ordinance and delivery platforms. The targeting staff should leverage the IO staff and resident technical expertise to accomplish this. Integrating OCI operations into the traditional force application process allows for the fullest synergistic effects of all the available capabilities. If planners wait until the Joint Targeting Coordination Board (JTCB) as stated in joint doctrine, they will lose the benefit of this effect and only achieve deconfliction. During this phase, targeteers need to insure organizations and units tasked to conduct OCIO have target materials they need to engage their respective targets. This requires that the existing Target

Material program be expanded to produce materials that contain new information such as antenna gain or network topography.

Execution

An important consideration in execution of OCI techniques is that they are not governed by the same factors as conventional force execution. The number of pilots and airframes, amount of ordinance, or time required to reach the target area do not limit OCIO. Data transmission speeds and automation technologies allow the potential to execute thousands of attacks near simultaneously. Targeteers must closely coordinate with the IO staff to ensure they are prepared to support this scope of effort. OCI mission folders are needed. Targeteers can not wait until assigned a target to collect the requisite mission data. Organizations need to maintain OCI target folders.

Combat Assessment

The main thrust of Information Operations (IO) Combat Assessment (CA) is the same as traditional BDA: Understand the objectives, know the target, comprehend the capabilities of the weapon and prepare collection assets to gather attack results. The application of certain IO weapons requires some adjustment to conventional CA thinking patterns. While no radical conceptual changes are needed, it is prudent to realize that, in certain circumstances, IO CA presents unique challenges to the analyst.

For the purposes of CA, one can divide IO into two distinct categories: kinetic and non-kinetic. Kinetic IO is essentially putting a bomb on a target with the intent of eliminating a specific function related to the commander's objective. Non-kinetic IO encompasses PSYOP, Deception, Electronic Warfare and Information Attack. It does not rely on conventional bombing to meet its objectives but uses many different mechanisms to affect a target. While the

overall analytical approach for CA of non-kinetic attacks remains the same, some adaptations are required.

In order to mitigate problems associated with non-kinetic IO, extensive preparation is required. An important part of this preparation is to establish closer working relationships with the operations community. Conventional JMEM/AS manuals provide a common reference to the operator and analyst. Because there is no similar reference document for non-kinetic options, the CA analyst must work very closely with information operations personnel to develop potential CA indicators.

Conventional terms may not lend themselves to certain aspects of non-kinetic IO and, in the worst case, IO situational analysis could be restricted by an insistence on using existing terminology. This is especially true when doing BDA analysis. The elements of existing CA methodology are logical and proven processes that are largely not affected by the differences between kinetic and non-kinetic IO. The absence of physical damage may require that CA will be based on the functional changes rather than the technical effect of the weapon on its target. The measurement of secondary or other follow-on effects will be the best available means to conduct CA in these cases.

The most significant change to the BDA procedures is the introduction of the term “Change Assessment”. Physical Change Assessment uses a complex understanding of target systems, intelligence capabilities, and IO weapons to identify and assess physical changes associated with the target. The quantitative extent of physical changes is used to assess the resulting functional changes. This assessment is not limited to the targeted target system, and may even encompass several systems in order to ascertain and justify the assessment results.

To quantify physical changes, the assessment is conducted using multiple indicators (battle damage indicators). Monitoring points are equipment, buildings, facilities or networks that will indicate functional or operational changes through specific physical changes. Physical changes can encompass a wide of spectrum outcomes from minimally increased/decreased activity or status of monitoring points up to the destruction of the selected target. Detecting physical changes requires looking at the right monitoring point to detect the correct indicators. However, an essential indicator can be easily overlooked if target development is incomplete, or if incorrect intelligence assets are used.

Traditional information sources, such as EO imagery, may not provide as much information for non-kinetic IO CA as they have in the past for conventional attacks. Depending on the IO weapon(s), complete IO combat assessment may require a combination of all available “INTS”. In order to reap all the benefits from our collection assets, it is critical to integrate CA needs at the very beginning of any IO planning phase, particularly the target development portion of the targeting cycle. Some collection assets are difficult to preposition and require long lead times. Additionally, much greater coordination must occur between IO planners and collections personnel to shorten collection response times. Another unknown is the process time needed to translate raw collector data into a useable form. All this must be part of the CA equation. In some cases, however, CNA techniques may have feedback sensors built-in to facilitate CA.

Current BDA reporting timelines are based on imagery receipt. Using imagery as the source, analysts determine physical damage using three criteria: Target type and size, warhead type and size, and warhead detonation location. Kinetic IO attack uses all of these for standard analysis and reporting. Non-kinetic attack presents a problem.

It may not be possible to use imagery for OCIO CA; therefore, imagery cannot drive timelines for some non-kinetic IO applications. Depending on the OCIO component, no physical damage may occur so it is necessary to modify BDA reporting procedures. Phase 1 report content must include physical change as well as physical damage. It is also important to note that, if physical changes do occur, they may not be detectable on imagery. Under the existing structure, it is possible that no initial reporting on non-kinetic IO will occur within conventional BDA channels.

Phase 2 reports are also keyed to imagery receipt for timeline starts. These reports are based essentially on additional analysis applied to Phase 1 reporting. If Phase 1 reporting is problematic, it may cascade throughout the BDA process and no functional BDA analysis may occur. In order to prevent this, an alternate means of generating Phase 2 reports needs to be developed based on an assessment matrix of physical changes. Analysts should be able to assess functional damage based on the sum of physical changes noted.

Non-Kinetic IO functional damage assessments rely heavily on the ability to measure numerous changes in activity at numerous locations. A target element vs. "INT" matrix, which documents changes in activity, can be used to simplify functional damage assessment, and justify the assessment's results. The matrix should be created during the target development phase due to the in-depth target system assessment and intelligence collection requirements. Targeteers will need to develop indicators that reveal status of target and weapon effectiveness during this phase. Collection and surveillance against the indicators will also need to be planned before attack.

Phase 3 reports are system assessments. Including results of non-Kinetic IO in these reports does not require any modifications since Phase 3 reports are a compilation of effects, not the

report of a specific attack. Although Combat Assessment is the final phase of the targeting cycle, the CA process must begin with the first phase--Objectives and Guidance. The "understandable, achievable, and measurable" objectives developed in the Objectives and Guidance phase will serve as the measurement device for mission success. Therefore, in all the phases of the joint targeting process, analysts must recognize the need to perform BDA/CA. This is especially true for the OCIO.

In some cases, despite advance planning, it will be very difficult to perform CA against targets of IO attacks. If CA can not be provided for a vital target, the commander may insist on hard kill against targets that have already been successfully engaged. In order to avoid this, potential IO targets should be selected with CA factors in mind.

Notes

¹ William Stallings, *Cryptography and Network Security: Principles and Practice*, 2d ed. (Upper Saddle River, New Jersey: Prentice Hall, 1999), 7

² Ibid

³ Ibid

⁴ Ibid

⁵ Ibid

⁶ Defense Intelligence Agency, *Information Operations Targeting (Draft)*, (Washington D.C., undated), 23.

⁷ Ibid.

⁸ Ibid.

⁹ Ibid.

¹⁰ Ibid.

¹¹ Ibid., 24.

¹² Ibid.

¹³ Depth is the measure of time from when a component is attacked and the affect felt. Cushion is the measure of the amount of a system's total capacity one needs to affect in order to achieve the desired effect. Reserve is a measure of stored capacity available within a system.

Part 4

Conclusions and Recommendations

It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change.

— Charles Darwin

Conclusions

Systematic Approach Required

Offensive counterinformation operations offer military planners new opportunities for achieving objectives in support of a JFC. These new opportunities rely on both old and new capabilities. Attacking a telecommunication switch with conventional weapons is an information attack relying on old capabilities. Increasing use of computer based information systems worldwide offer opportunities for new capabilities to attack computer networks. That same telecommunication switch could be affected by an information attack. While there is a great deal that is new in the arena of information operations, OCI still requires a systematic approach to translate the commander's objectives into actionable entities that can be affected to achieve these objectives. In addition, commanders are going to want to know what the probability of achieving the desired effect is, and will want feedback as to whether or not the objective has been obtained. Successful employment of offensive counterinformation operations requires the same process as the traditional forms of military force. Planners need to establish objectives,

identify targets, recommend capabilities, apply these capabilities and assess the level of success of the application of these capabilities.

Joint Targeting Process

When one places OCI within the context of theater operations plans, it is easy to see that the existing process for translating the commander's objectives into targets is analogous to the requirement for employing OCI. The joint targeting process provides a conceptual model that translates the commander's objectives into targets that can be attacked taking into account operational limitations. Targeteers analyze these targets for specific vulnerabilities taking into account actual capabilities. Once targets and capabilities are analyzed, one can make recommendations about the optimum matching of targets with capabilities. Once the commander decides on a course of action and it is executed, analyst must provide the commander a continuing assessment of what effect the plan has achieved.

Offensive Counterinformation Targeting Process

Personnel planning OCIO can use the existing joint targeting process with only minor modifications. However, there remains much work to do. As was pointed out, the intelligence requirements for OCIO are much greater. In addition, seven recommendations are addressed below.

Recommendations

The primary purpose of this paper is to assist both targeteers and IO planners in making use of evolving capabilities. During the research for this paper, several procedural issues surfaced which must be resolved to meet that goal fully. These recommendations are listed in Table 1 below.

Table 2. Recommendations

1. Develop Information Operations Target Materials
2. Develop Information Operations Critical Elements of Generic Installations
3. Develop Target Folder Requirements
4. Develop Joint Information Operations Weaponing Methodologies
5. Fully Integrate Information Operations with Other Operations
6. Ensure Adequate Access
7. Refine Information Operations Terminology

Develop IO Target Materials

Target materials must be developed that support IO planning and execution. While there are several efforts underway to develop databases to support the full spectrum of IPB, an additional step is required for these products to be considered “target materials”. Target materials are highly standardized products that are certified to have sufficient accuracy for mission planning and execution. Existing product lines, such as the Basic Target Graphic (BTG) need to be modified and new products developed. Specific requirements need to be derived from the IO community.

Develop IO Critical Elements for Generic Installations

DIA’s Critical Elements of Selected Generic Installations Handbook needs to be updated to include target elements not traditionally considered in the past. This baseline reference has extensive data on the physical makeup of facilities, but does not address other aspects of

installations that could be exploited through non-kinetic means. The handbook must include data that would support target development and weaponeering for nontraditional options. For example, the computer networks associated with a particular type of facility need to be described in detail.

Develop IO Target Folders Requirements

Target folders must be capable of supporting all potential operations, not just application of kinetic weapons. Targeteers must work with IO planners and operators to determine exactly what is required to support their mission. Folders must be designed and ready before execution. The potential need to support multiple different venues (physical destruction, information attack, EW, etc.) may require “virtual target folders” resident on electronic databases.

Develop Joint IO Weaponeering Methodologies

A joint methodology is needed to compare projected effectiveness of IO capabilities. This will allow decisions-makers to make informed decisions on the optimum use of these or traditional techniques. Targeteers must be able to provide the IO equivalent of “probability of destruction” in a reliable and repeatable format. A methodology and body of data similar to the JMEMs must evolve over time in order to “mainstream” non-kinetic IO techniques along with the long-standing kinetic options.

Fully Integrate Information Operations with Other Operations

Optimal application of IO requires better coordination between planners working on traditional planning, and those involved in planning for non-traditional capabilities. The IO Cells must work very closely with the Targeting Cells at all levels.

Ensure Adequate Access

Certain aspects of IO require protection in strict security channels. While recognizing this limitation, only information that must be truly protected at higher levels should be restricted. Other elements need to be provided to the traditional targeting intelligence and operational planning community in order to reduce stovepiping of IO capabilities. To facilitate this, Special Information Operation (SIO) managers should develop a set of data, which they can share outside of restricted channels.

Refine IO Terminology

Terms associated with both IO and targeting need to be more discretely defined. Notions such as kinetic and non-kinetic IO, and the very concept of a target, must be further explored to address completely IO and targeting as a part of Joint Doctrine and Strategy. Terminology such as Computer Network Attack must be refined in order to ensure there is no overlap with other aspects of IO such as Physical Destruction or Electronic Warfare.

Summary

These specific recommendations, if implemented, will improve the US military's ability to conduct offensive counterinformation operations. They are really only the first steps in moving OCIO from theory to an operational capability. The fact that tools exist today, and yet we do not have an adequately evolved process for planning and incorporating OCIO into our current operational planning process is a situation that must be rectified. All these recommendations must be acted on now. As we enter a new century, to paraphrase Charles Darwin we should remember that **it is not the strongest military that survives, nor the most technological, but the one most responsive to change.**

BIBLIOGRAPHY

- Adams, James. *The Next War: Computers are the Weapons & the Front Line Is Everywhere*. New York: Simon & Schuster, 1998.
- Anonymous. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, 2nd ed. Indianapolis, Indiana: Sams Publishing, 1998.
- Black, Uyles. *Emerging Communications Technologies*, 2nd ed. Upper Saddle River, New Jersey, 1997.
- Brenton, Chris. *Mastering Network Security*. San Francisco: Sybex Network Press, 1999.
- Broolshear, J. Glenn. *Computer Science, An Overview*, 5th ed. Reading, Massachusetts: Addison-Wesley, 1997.
- Cheswick, William R. and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, Massachusetts: Addison-Wesley, 1994.
- Dalton, Jane and Jim Hauck. "IO and International Law". Briefing given by the Deputy Legal Councils to the CJCS to Joint Staff Information Operations Targeting Working Group May 1998.
- Defense Intelligence Agency. *Targeting and Information Operations*. Draft Defense Intelligence Reference Document, April 1999.
- Denning, Dorothy E. *Information Warfare and Security*. Reading, Massachusetts: Addison-Wesley, 1999.
- Denning, Peter J, ed. *Computers Under Attack: Intruders, Worms, and Viruses*. Reading, Massachusetts: Addison-Wesley, 1990.
- Department of the Air Force. *Cornerstones of Information Warfare*. Washington D.C., undated.
- _____. *Information Warfare: (The IW Primer)*. Washington D.C., 1995.
- _____. *Air Force Intelligence and Information Warfare*. Washington D.C., 1996.
- _____. *Air Force Doctrine Document 1, Air Force Basic Doctrine*. Washington D.C., 1997.
- _____. *Air Force Doctrine Document 2, Organization and Employment of Aerospace Power*. Washington D.C., 1998.
- _____. *Air Force Doctrine Document 2-5, Information Operations*. Washington D.C., 1998.
- Dodd, Annabel Z. *The Essential Guide to Telecommunications*. Upper Saddle River, New Jersey, 1998.
- DPL: Professional Decision Analysis Software, DPLf User Manual. Applied Decision Analysis LLC (ADA), 1998.

- Goldberg, Mike. "Intelligence Law: The Legal Restrictions on Information Operations/Warfare." Briefing given by the 67 IW/JA, undated.
- Haertling, Kenneth P. Implementing Information Warfare in the Weapon Targeting Process. Air Force Information Warfare Center, Systems Analysis Directorate, 1997.
- Pfleeger, Charles P. Security in Computing, 2nd ed. Upper Saddle River, New Jersey: Prentice Hall PTR, 1997.
- Schwartau, Winn. Information Warfare: Chaos on the Electronic Super Highway. New York: Thunder's Mouth Press, 1994.
- Shimomura, Tsutomu and John Markoff. Take Down: The Pursuit of Kevin Mitnick, America's Most Wanted Computer Outlaw -- By the Man Who Did It. New York; Hyperion, 1996.
- Stallings, William. Cryptography and Network Security: Principles and Practice, 2nd ed. Upper Saddle River, New Jersey: Prentice Hall, 1999.
- Stoll, Cliff. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Pocket Books, 1989.
- Wang, Wallace. Steal This Computer Book: What They Won't Tell You About the Internet. San Francisco: No Starch Press, 1998.
- Williamson, Charles A. Psychological Operations in the Information Age. Unpublished and undated paper presented to Joint Staff Information Operations Working Group in 1999.
- Zorn, Wayne. Implementing Information Operations in the Targeting Process: Measures of Effectiveness Methodology Electronic Warfare (Electronic Attack). Air Force Information Warfare Center White Paper, 1998.