

LESSON 7

INTRODUCTION TO INFORMATION OPERATIONS

“We live in an age that is driven by information. Technological breakthroughs...are changing the face of war and how we prepare for it.”

— William Perry, Former Secretary of Defense

Lesson Introduction

Many would say the face of war has already changed. Technology and the use of information and information technologies have already had a significant impact on military operations. But what is “Information Operations (IO)”? Is it a subset of C4? Is it the same as cyber warfare? Does physical destruction have a place in IO? These questions are difficult to answer. Defining IO has been a problem for the Joint Staff and the Services. Currently, Joint Pub 3-13 and the DoD Dictionary, Joint Pub 1-02, still contain doctrinal IO definitions that will be discussed later in this lesson. IO continues to evolve. Current Joint doctrine approaches IO from offensive and defensive perspectives, which will both be discussed in requirements two and three.

In the near future, the nation will face a wide range of interests, opportunities, and challenges and will require a military that can both win wars and contribute to peace. The global interests and responsibilities of the United States will endure, and there is no indication that threats to those interests and responsibilities, or to our allies, will disappear.

Potential adversaries will have access to the global commercial industrial base and much of the same technology as the U.S. military. We will not necessarily sustain a wide technological advantage over our adversaries in all areas. Increased availability of commercial satellites, digital communications, and the public Internet all give adversaries new capabilities at a relatively low cost. Other critical aspects, and often forgotten in the prosecution of IO, are the history, culture, religion, and language of the adversary. Our lack of a basic understanding of our adversary can negate all the applications of technology, systematic analyses, and targeting efforts conducted by U.S. forces.

In this lesson you will be given an overview of IO from the operational level of war perspective. You will learn what Marine Corps doctrine says about decision-making and how information is stratified. You will be exposed to Joint doctrine about offensive and defensive IO. Lastly you will read the Marine Corps’ concept of IO and how IO affects operations of Marine Corps forces. In 8806A, the Joint and Multinational Operations course, you will get into more details about IO, especially from the Marine Corps doctrinal perspective.

Student Requirements by Educational Objective

Requirement 1

Objective 1. Understand how the Observe, Orient, Decide and Act (OODA) Loop Model and the Information Hierarchy relate to information operations (IO). [JPME Area 2(d)]

Objective 2. Understand the basic doctrine and planning considerations associated with IO at the operational level of war. [JPME Area 2(a), 4(e), 5(a)(b)(c)(d)]

Read:

- MCDP 6, *Command and Control*, pp. 63 to 71 (9 pages)
- *Response to “The Air War Over Serbia” Initial Report* provided by the Air University (2 pages)

View:

- DOCNET segment, *Joint Doctrine for Information Operations*, “Introduction.” (21 minutes) Refer to Joint Pub 3-13, 9 October 1998, pp. I-1 to I-20

As new information technologies, systems, and procedures make the same detailed information available at all levels of the chain of command, leaders must understand the implications for decision-making processes. If one accepts the OODA Loop Model of decision-making, and command and control, then IO is a method to disrupt an adversary’s decision-making or command and control by interrupting or slowing down the speed at which the OODA Loop is functioning. The cycle might not be completely broken by our IO efforts, only disrupted for a necessary amount of time to enable other kinds of military operations to achieve some success, potentially decisive success. Since the OODA loop serves to create a cohesive mental image for a decision-maker, disruption of the loop might distort that image enough to cause a bad decision thus creating a friendly advantage or opportunity. When applying IO, one must look at the Information Hierarchy to determine which level the IO effort affects. If IO only focuses on the lower end of the hierarchy, such as raw data, then one must expect to achieve less effect on decision-making. On the other hand, in order to affect the knowledge and/or understanding levels of the hierarchy, coherent and consistent application of IO will be critical to ensure believability and effectively cloud the adversary’s mental image and situational awareness. Again, the ultimate goal is to negatively affect the adversary’s decision-making. We must understand that certain variables that affect an adversary’s ability to understand is outside our sphere of influence. We cannot change the decision-maker’s intellectual ability, his education, his experiences, or the cultural and religious influences that affect how he thinks. There are serious limitations to IO.

Below is a list of current doctrinal definitions of IO terminology:

information — 1. Facts, data, or instructions in any medium or form. 2. The meaning

that a human assigns to data by means of the known conventions used in their representation.

information operations — Actions taken to affect adversary information and information systems while defending one's own information and information systems.

information superiority — That degree of dominance in the information domain, which permits the conduct of operations without effective opposition.

information system — The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

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

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

computer network defense (CND) — Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

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

electronic warfare (EW) — Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

military deception — Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the

accomplishment of the friendly mission. The five categories of military deception are as follows.

- Strategic military deception
- Operational military deception
- Tactical military deception
- Service military deception
- Military deception in support of operations security

operations security (OPSEC) — A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems
- Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Requirement 2

Objective 3. Understand the basic doctrine and planning considerations associated with offensive IO at the operational level of war. [JPME Area 2(a), 4(e), 5(a)(b)(c)(d)]

View:

- DOCNET segment, *Joint Doctrine for Information Operations*, “Offensive Information Operations.” (14 minutes) Refer to Joint Pub 3-13, 9 October 1998, pp. II-1 to II-15

As with all other types of planning, developing an IO employment plan starts with a complete and thorough understanding of the JFC’s mission, concept of operations, objectives, and intent. The IO plan at the Joint level must be carefully and appropriately integrated with applicable diplomatic, economic, and military efforts in order to ensure harmony and synergy. The following is a list of important IO planning considerations.

- IO planning usually requires long-term development and must often consider peacetime circumstances and situations to be effective.
- Establishing the organization of subordinate forces and designating command relationships in order to achieve IO unity of effort is especially important. This effort will usually require interagency agreement on synchronization, coordination, and deconfliction of the IO execution phase.

- Planners will be required to identify Service, Joint, and interagency IO capabilities early on in order to provide the JFC with a “tool box” approach to developing his plan.
- Identifying the adversary’s strategic and operational IO centers of gravity (COG) is critical. However, because the IO portion of the IPB differs from the other, more traditional parts, planners should expect greater lead times and expanded collection requirements to identify these COGs.
- Adherence to a common level of protection throughout the command structure is an essential yet obviously monumental task. Determining the scope of what needs to be protected and the standards for how much protection is required is a huge challenge for the JFC and his staff.

Requirement 3

Objective 4. Understand the basic doctrine and planning considerations associated with defensive IO at the operational level of war. [JPME Area 2(a), 4(e), 5(a)(b)(c)(d)]

View:

- DOCNET segment, *Joint Doctrine for Information Operations*, “Defensive Information Operations” (14 minutes). Refer to Joint Pub 3-13, 9 October 1998, pp. III-1 to III-15

Requirement 4

Objective 5. Comprehend the Marine Corps concept of IO and understand how it relates to Joint doctrine. [JPME Area 2(d)]

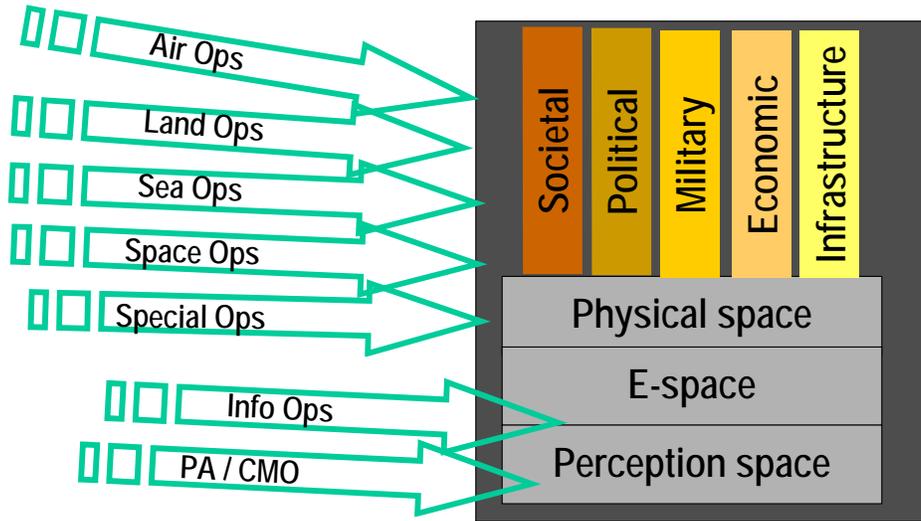
Read:

- *A Concept for Information Operations*, 19 April 2002, pp. 5 to 15 (10 pages)

Joint staffs and Service staffs view IO in the Joint environment differently. Since IO begins at the national level and is often buried at the higher levels of security classification, implementation of IO at the operational level of war becomes difficult. Joint forces may be witting or unwitting participants in a national IO campaign. Attempting to develop doctrine to support such operations depends upon the context of the force or forces implementing such operations. It is natural that individual Services perceive IO differently since they all see the battlespace from different perspectives. Some view the current doctrinal definition of IO as being too broad and, thus, allowing almost everything to be called IO. Some recognize that IO offers a unique arsenal of tools or capability sets, many of which can be used effectively in peacetime as well as in conflict. Some also feel we need to clarify the relationships between military IO, public affairs, and public diplomacy in the U.S. government information campaign. Regardless, military forces will be called upon to execute certain aspects of IO, whether clearly

defined or not. Military forces will be called upon to effectively integrate IO into a larger campaign. The slide below offers a graphic depiction of this notion.

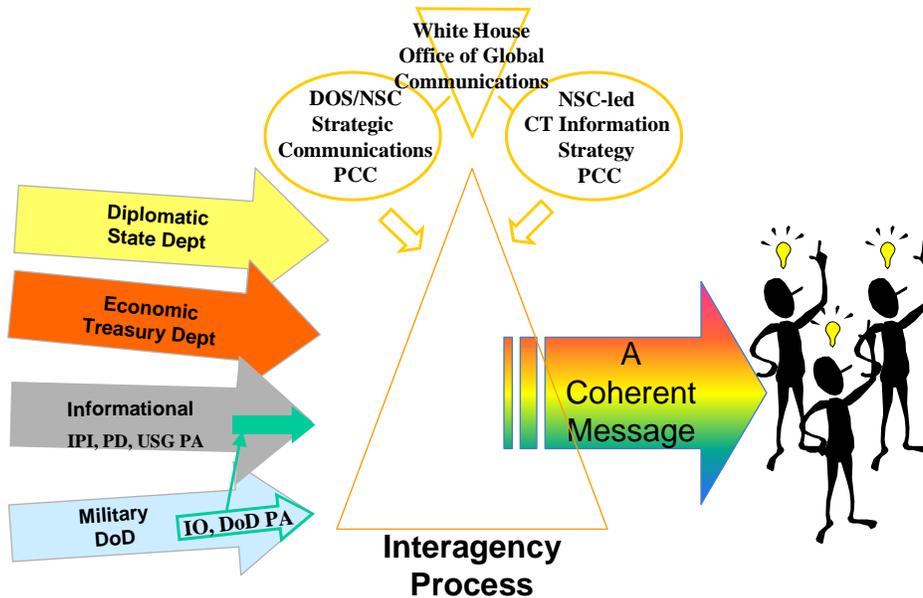
IO Integrated Into Military Operations



Campaign Execution

The slide below also suggests how to organize the information campaign at the national level.

Organizing the Information Campaign -- The Solution



According to the Marine Corps concept of IO, IO can be used to influence peacetime periods by, deterring during pre-crisis, enabling during crisis, and restoring during post-crisis across the spectrum of diplomatic, economic, military, and social elements of national power. IO conducted by MAGTFs will consist primarily of battlespace shaping, force enhancement, force protection actions and any other information-oriented activity that the MAGTF can leverage to better facilitate the application of combat power.

Battlespace Shaping. During crisis, MAGTF-shaping operations must be linked to U.S. strategic objectives and must be consistent with ongoing regional engagement activities. During shaping operations, it must be recognized that the targeting means is secondary to achieving the desired targeting effect, especially since “targets” in IO terms will no longer reside solely in the physical domain but will include the perceptions and actions of civilians, key leaders, and our military foes.

Force Enhancement. In many ways, the ability to obtain timely and accurate information has emerged as a critical aspect of command, control, strategic agility, and operational maneuver. The force that best controls, uses, and safeguards information and information systems has always possessed a decided military advantage; this fact will not change. During conflict, the MAGTF may rely heavily on electronic warfare, military deception, influence operations, and physical destruction to attack command and control, intelligence, and other critical information-based processes that directly impact an adversary’s ability to conduct military operations. Capabilities outside the Marine Corps include computer network attack, psychological operations, and the means to manage media attention on the operation.

Force Protection. The MAGTF commander will depend on information to plan operations and employ his forces. Information systems enable and enhance warfighting capabilities; however, our increased dependence on these rapidly evolving technologies will create new vulnerabilities. The integration of protection, detection, and reaction capabilities is needed to mitigate the effects of enemy action and environmental effects. Defensive IO encompasses four interrelated processes: information environment protection, attack detection, capability restoration, and attack response.

IO will complement the Marine Corps’ pursuit of Expeditionary Maneuver Warfare (EMW) aims by enhancing operational maneuver and force protection, by expanding knowledge and understanding of the environment and its cultures, and by providing the means to extend the influence of the MAGTF well beyond the range of its weapons systems.

Lesson Summary

Some will argue that IO is too complex a form of warfare. The counter to this is (1) we live in the information age with all its implications and (2) nations and businesses already conduct various forms of IO to gain advantages over competitors. To ignore the

possibilities, dangers, and implications of IO is the moral equivalent of ignoring the use of the airplane as that technology developed during the early part of the 20th century.

IO comprises many of the functions we have always performed in the past; PSYOP, EW, OPSEC, deception, physical destruction (of selected information systems), etc. What is new are the technologies employed (for example, information driven systems and weapons) and some of the adversary’s vulnerabilities (C2 systems, telecommunications, air traffic control, business applications, etc.). As this form of warfare continues to evolve, we must remain mindful that the purpose of IO is to negatively affect the adversary’s decision-making and command and control to enable the U.S. to successfully defend and promote its national interests and responsibilities.

JPME Summary

AREA 1					AREA 2				AREA 3					AREA 4					AREA 5			
A	B	C	D	E	A	B	C	D	A	B	C	D	E	A	B	C	D	E	A	B	C	D
					X			X										X	X	X	X	X