

Unit Introduction

Advances in technology continue to change the way wars are fought around the world. As we explored in the Public Affairs History unit of instruction, technology has had a profound impact on how we fight and share information. Information flows faster than ever before.

E-mails, digital images, satellite uplinks, cell phones, digital video cameras, 24-hour news channels, streaming video, and many other communication mediums have all had an impact on how we communicate with the public and our allies. It also presents challenges to how we secure information on the battlefield.



The increasing worldwide reliance on information cannot be emphasized enough, and will continue to grow exponentially. In addition, more and more people are getting news and information from sources other than news outlets. The U.S. military is an industrial age military making the transformation to digital age war fighters. Arising from this realization, the Department of Defense has embraced the concept of Information Operations (IO). IO is not new to the DOD, but has been revised within the last ten years to meet modern communication and war fighting challenges. In this unit, we will introduce you to IO and discuss the role of public affairs within the IO working group.

Unit Introduction



Public affairs practitioners are key players in the information age. Practitioners use various modes of communication to talk with the multitude of audiences we try to inform. Public affairs is a vital component of Information Operations in coordinating with various audiences.

This class will give you a brief introduction into IO from the Joint services perspective. The basic references for material presented in this unit are DOD Directive O-3600.01 and Joint Pub 3-13, Joint Doctrine for Information Operations. However, understand each service will have its own ideology and practice of information operations, so you should consult service specific information about IO. Also understand that IO is fluid and continually evolving.

Public Affairs is considered a related function of IO and not a core capability.

We will discuss the difference later in this unit; however, there are no "pat" answers to how public affairs coordinates and functions within IO. Joint Publication 3-13 outlines the role of public affairs within Information Operations.

Additionally, Combatant Commanders adjust IO to work in a theater of operations. The "final word" on how IO works in the joint environment is not out there yet.

Objectives

Given an information operations scenario, develop and recommend public affairs support for Information Operations related to the scenario in accordance with Department of Defense and service public affairs policies and regulations. Upon completion of this unit of instruction, the student will be able to:

- Define computer network attack
- Define information assurance
- Define information-based processes
- Define information environment
- Define information operations
- State the two major subdivisions within information operations
- Define the term information superiority
- Define the term information system
- Define the term information warfare
- Define the term special information operations
- State the five public affairs activities that support offensive Information Operations
- State the purpose of the public affairs representative in an Information Operations cell

Unit Overview

In this unit, we will review:

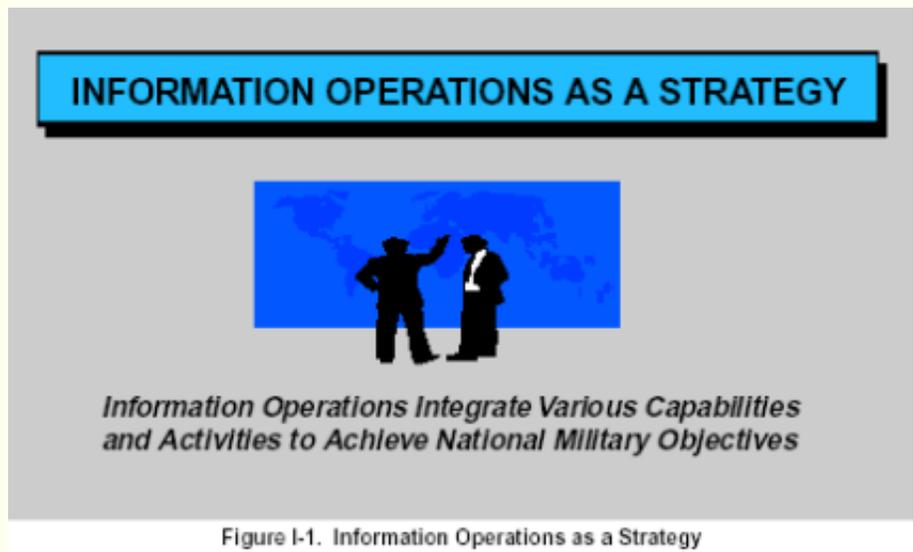
- Definition of Information Operations
- History of Information Operations
- The two major subdivisions within Information Operations
- Information Operations capabilities
- Information Campaign
- Public Affairs activities that support Information Operations
- The role of Public Affairs in an Information Operations Cell
- Myths about Public Affairs and Information Operations
- Implications for the Future

Definition

The broad Joint definition of Information Operations can be found in Joint Pub 3-13, but simply stated IO is "...actions taken to affect adversary information and information systems while defending one's own information and information systems."

A successful IO campaign requires all components to integrate and work together. It also requires integration of offensive and defensive capabilities, which we will discuss later, and activities.

Successful IO also must work with intelligence support.



The goal of Information Operations (IO) is to ensure that we don't have war. First and foremost, IO is strategically used as a deterrent to armed conflict. However in times of crises and armed conflict, Information Operations becomes known as [Information Warfare \(IW\)](#). IO/IW then becomes a force multiplier.

Definition of Civil Affairs

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

Definition of Psychological Operations

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

History

The story of information warfare has followed and sometimes led societies. Starting way back in written world history, some of the first conveyors of information were lanterns or flags. Many of us know the story of Paul Revere's Ride: one (lantern) if by sea, two (lanterns) if by land. The lanterns were lit in the church steeple, which wasn't anything unusual to the British, but was a signal to colonists that "The British are coming, the British are coming." This is an early example of information warfare, although it wasn't called that back then.



Through the centuries, it progressed through mirrors, mail and towers. The advent of the telegraph greatly expanded the lines of communication and distance. As we can see, starting at the point when radios became popular, the curve in the last few years has been almost straight up, and continues its vertical climb.

In the early '90s, armed forces leaders realized that the power of information was equal in importance to economic, political and military power. Now, it could be considered that the power of information is often greater than the other three elements. In fact, it may be said if information operations fail, then the other instruments of national power are not likely to achieve their objectives.

Information Campaign

What is an Information campaign? The Campaign of words, images and perceptions. Remember that these words, images and perceptions are used in Information Operations and Information Warfare. A campaign is planned with a total effort in mind. It is strategic, operational and tactical in scope.

Look at the chart on the right. In situations of potential armed conflict, policy makers establish the objectives and themes for an information campaign as necessary. They begin as diplomatic initiatives and work their way along a continuum of action.

Information Operations Objectives has become an important instrument of power. Joint Publication 3-13 has categorized IO as having four focus elements: Diplomatic, Informational, Military and Economic (DIME). We must use them all to be successful.



Figure II-1. Examples of Information Operations Objectives

Coordinating the Information Campaign

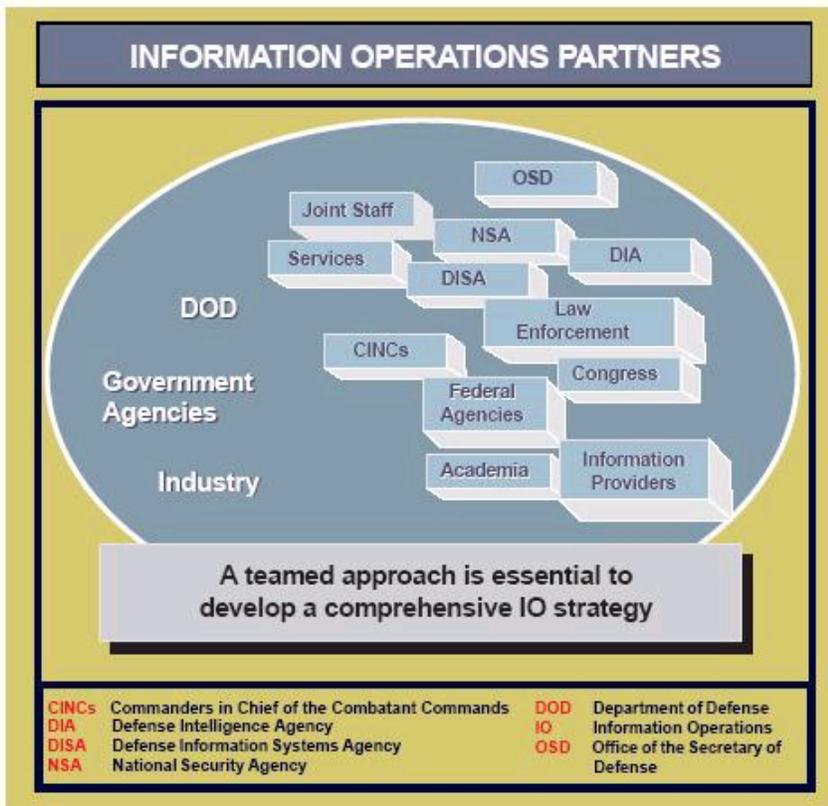


Figure I-5. Information Operations Partners

The success of any campaign hinges on coordination with U.S. government global communications across multiple agencies. Thus, the U.S. military is a key component of IO.

We've already talked about Information Operations as a deterrent to war and coordination with multiple agencies. On a macro level Information Operations requires coordination between various agencies. In order to succeed with the DIME concept, IO includes other federal agencies.

Before the United States invaded Iraq after 9/11, President Bush gave warnings to Saddam Hussein to comply with weapons inspectors and to turnover its weapons of mass destruction Iraq kept as reported through the national and international intelligence community. The ultimatum was that the United States would invade if Hussein did

not comply. This is a very simple summary of events, but we use this to illustrate the use of Diplomacy (U.N. weapons inspectors), Informational (intelligence reports), and Military (the eventual invasion of Iraq) in this scenario.

Another example that highlights the Economic effect is the trade embargo on Cuba for being a communist country. These Information Operations are to deter war and achieve an objective without using military troops. Sometimes it works, sometimes it doesn't.

Information Campaign

When a strategic level IO campaign doesn't work, when diplomatic and deterrent objectives fail and military action is required, then IO moves to operational level objectives. That's when the military becomes involved.

Military IO supports the entire "Information Campaign" ... but primarily achieves theater military objectives.

Joint Pub 3-13 defines military IO as planning an information campaign that includes the Joint Forces Commanders' mission, concept and operations objectives and intent in coordination with air, land, and sea power, special operations, the strategic, operational and tactical as well as the economic and diplomatic.

There are several separate capabilities and activities that comprise of the total military effort, however, there are five IO core capabilities.

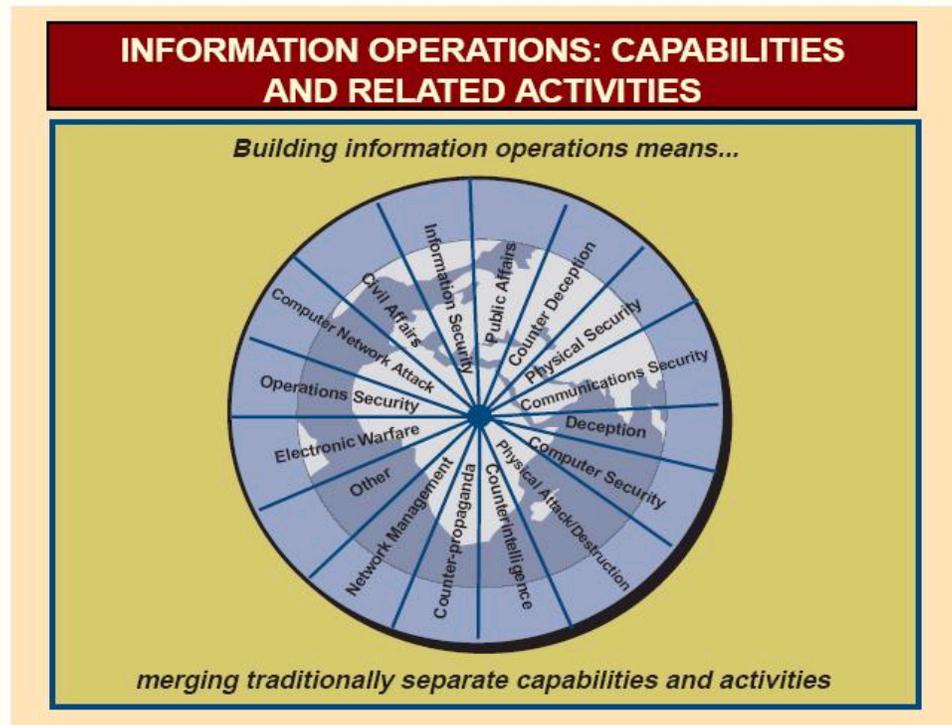


Figure I-3. Informations Operations: Capabilities and Related Activities

Information Operations Capabilities

The five core capabilities of IO, which incorporates all military communication capabilities are:

- Computer Network Operations (CNO), which includes [Computer Network Attack \(CNA\)](#).
- Psychological Operations (PSYOPS)
- Electronic Warfare (EW)
- Military Deception (MD)
- Operational Security (OPSEC)

There are also three supporting capabilities:

- [Information Assurance](#)
- Physical Security
- Counterintelligence, which includes counter deception and counter propaganda.
- Combat Camera
- Physical (Kinetic) Attack

Additionally, there are three related capabilities of counter propaganda: public affairs, civil-military operations, and Defense Support to Public Diplomacy. In Unit 11 we discussed public affairs and civil-military operations roles in IO, but one thing to keep in mind throughout this unit is that public affairs and PSYOPS must remain separate. It is the reason PA is a related capability.

Note: You need to be aware of each capability, but you need to know the public affairs role within the spectrum of IO capabilities.

However, each capability – core, supporting, or related – plays a role in two IO subdivisions: offensive and defensive information operations.

Major Subdivisions - Offensive IO

Offensive IO is the integrated use of assigned and supporting capabilities and activities, mutually supported by the intelligence, to affect adversary decision makers and achieve or promote specific objectives.

Examples: OPSEC, military deception, PSYOPS, Electronic Warfare (EW)

[Computer Network Attack](#): Operations to disrupt, deny, degrade, or destroy information resident in computer and computer networks or computers and networks themselves. This is the type of function you find IT divisions.

[Special Information Operations](#): IO that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to national security of the United States, requires special review and approval process.

Major Subdivisions – Defensive IO

Defensive IO is the integrated and coordinated policies and procedures, operations, personnel, and technology designed to protect and defend information and information operation systems.

Examples: Physical security, EW, Counter-Propaganda (Where public affairs plays a vital role in IO)

Emphasis can be both offensive and defensive, such as EW and special information operations.

Information Assurance: IO that protects and defends information systems by ensuring their capability, integrity, authentication, confidentiality, and non-repudiation. This includes restoration systems by incorporating protection, detection, and reaction capabilities.

We have discussed the basic concepts and background of IO. How does all of this information relate to each other? We are going to take a look at putting it all together for an Information Campaign.

Global Information Environment

We have all heard terms like "Information Age" and "Information Superhighway" to describe the growing influence information has had on our society.

In the context of IO, it is called the Global Information Environment. The Global Information Environment is "all individuals, organizations or systems, most of which are outside the control of the military ... that collect, process, and disseminate information to national and international audiences."

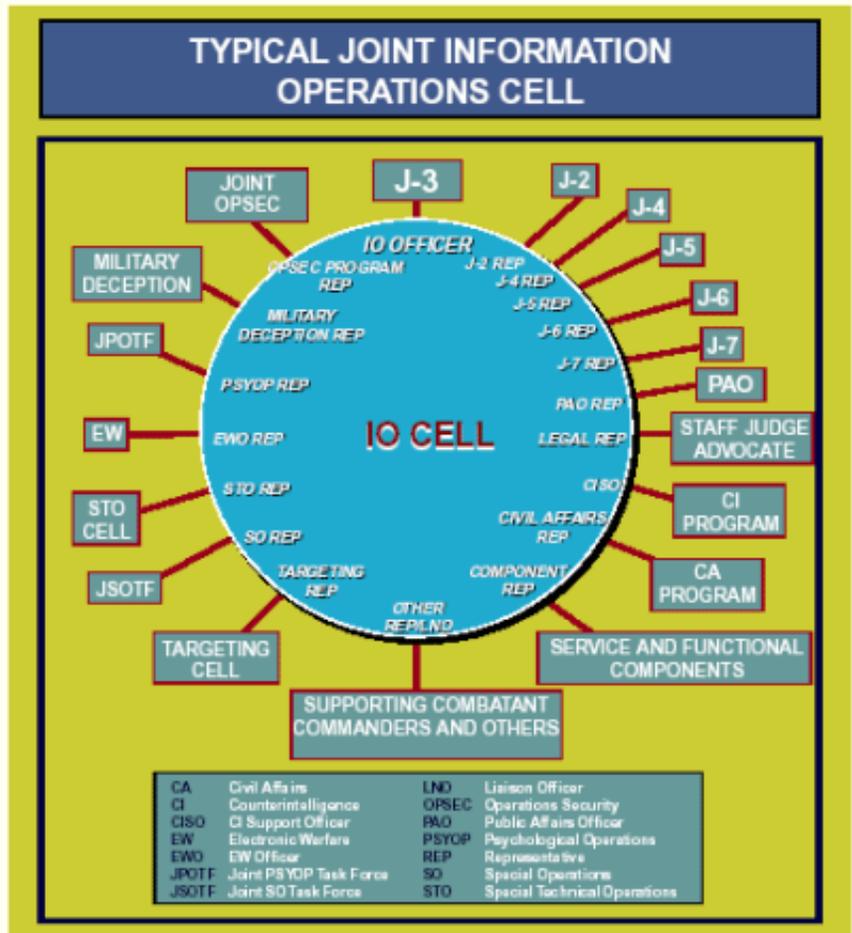


Figure IV-1. Typical Joint Information Operations Cell

Public Affairs Activities that support Information Operations

Public affairs is related to IO because of our involvement in the Global Information Environment. We disseminate and process information that supports IO in the following areas:

- Expedite flow of accurate, timely information to internal/external audiences
- Create awareness of military goals in operations, campaigns
- Satisfy desires of internal/external audiences to be kept informed
- Inform internal/external audiences of significant developments affecting them
- Through the media, inform adversary or potential adversary about friendly force's intent/capability

Public affairs should coordinate with IO to ensure unity of effort with messaging. In addition, we must safeguard our operations against the offensive communication threats facing us in a conflict. The way we do that is with a Information Operations Working Group (IOWG).

This is a way for practitioners to be part of an IO Cell without jeopardizing your commander and unit's credibility or their relationship with the public's trust. You must remember that public affairs is a command responsibility . A PA will advise his commander, but, ultimately, we carry out the commander's intent. We will talk in more detail about what public affairs does specifically to support PSYOPS and Civil Affairs as part of an Information Campaign in later units of instruction. For now, lets examine a broad perspective of PA and IO.

Role of Public Affairs in an Information Operations Cell

PA expedites the flow of timely and accurate information about the activities of U.S. joint forces to the public and internal audiences. Simply put, PA supports IO by doing our job.

Public affairs also is responsible for gaining or sustaining support for the U.S. and coalition position, with the objectives of:

- Reducing the need for combat
- Influencing events with non-lethal means
- Countering propaganda and disinformation
- Discouraging adversary offensive operations
- Deterring hostile actions
- Undermining illegitimate regimes
- Supporting the maintenance of coalitions

Public affairs is a related capability because practitioners disseminate truthful information where other capabilities within IO deal with deception. Coordination of IO and PA is critical to the commander and a successful campaign. Without robust PA support IO will not be successful.

Role of Public Affairs in an Information Operations Cell

PA is to provide a Joint Forces Command 14 Paragraph Annex F, in accordance with Joint Publication 3-13, to support an information campaign. In the Annex F unit of instruction we briefly talked about the JCS format, but here is a reminder of the format:

14 Paragraph Annex – This format is most often used at JCS level of strategic planning. For this reason, it is beneficial to be familiar with it because you might have to put it into action. You will most likely not use it at lower levels within DOD but you may have to incorporate some elements of it as operational guidance from higher headquarters.

JCS Format

1. Situation
2. Mission
3. Execution
4. Concept of the operation
5. Tasks
6. Coordinating instructions
7. Accreditation
8. Field press censorship
9. Arrangements for the media
10. Security of operations & personnel
11. Operational security
12. Audiovisual and visual information
13. Internal information
14. Community relations

Your job as a PAO or PA representative in an IOWG is to provide counsel and coordination on internal, external and command information.

Concerns about Public Affairs Relationship to Information Operations

As you go out and encounter IO in the field, you will meet practitioners who are skeptical and apprehensive about IO. Most of what you will hear are concerns about PA's involvement with IO, which include:

- PA will lose its direct access to the commander if involved with IO.
- PA will become a part of IO, and therefore report directly to IO "chief" who may not understand PA and what we can/can't do.
- PA will be associated with deception and PSYOP, and therefore lose our credibility with the media and other external/internal audiences.

Former Chairman of the Joint Chiefs of Staff Gen. Richard B Myers, U.S. Air Force, addressed these concerns with a [memo](#) concerning public affairs relationship with Information Operations.

PA activities will NOT be used as a military deception capability or to provide DISINFORMATION to either internal or external audiences.

Implications for the Future

Information Operations is still growing in the military. This concept will continue to grow and redefine itself as the Department of Defense uses lessons learned and best practices to improve efforts. Some of the things you can expect to see with public affairs' role in IO are:

- Increased coordination between PA and CA; PA and PSYOPs
- Rise of a professional IO career path
- Increased use of Virtual Force Projection
- Images are stronger than words
- Must better understand and get ahead of enemy propaganda
- Must be able to anticipate and get bad news out first - before the enemy puts his "spin" on it
- Better understand the increasing use of Internet by friend and foe and the media's dynamics of news reporting
- Realities of the GIE - technology & the demand for news
- Must be able to carefully coordinate and orchestrate IO/PA ops across oceans and time zones; "Virtual Force Projection"
- Must be "offensive" to win the Information Battlespace!

Credibility and truth are inseparable. PAOs operate in the truth. Everything we say must be true. We must continue to be "credibility custodians."

Unit Summary

This unit of instruction was meant to give you an overview of Information Operations and the role that public affairs plays in supporting an information campaign. We have discussed:

- Definitions of Information Operations, Civil Affairs and Psychological Operations
- History of Information Operations
- The two major subdivisions within Information Operations
- Information Operations capabilities
- Information Campaign
- Public Affairs activities that support Information Operations
- The role of Public Affairs in an Information Operations Cell
- Concerns about Public Affairs and Information Operations
- Implications for the Future

Unit Summary

We have entered the information age. You are the lead warriors when it comes to information and the battlefield. It is no longer "OK" to sit outside the IO circle. It is imperative you understand Information Operations so that you can contribute to the information warfare efforts.