Objectives in the Information Environment

By Marc Romanych, Major USA (Retired) and Robert Cordray III

Editorial Abstract: *1st IO Command's Marc Romanych and Robert Cordray provide recommendations how to more precisely define objectives and effects for information operations and propose a methodology focusing on Objective, Target, Function and Purpose.*

The practitioners of information operations (IO) have a nagging problem – namely how to clearly describe objectives and effects in the information environment. To date, neither doctrine nor practice has solved this matter. A review of Joint and Service doctrine publications as well as recently published IO plans demonstrates the magnitude of the situation.

Although much is written about effects, emerging and current Joint targeting and IO doctrine skirt the issue. Doctrine tells us that effects are supposed to be specific, quantifiable, and measurable. Yet, there is no established set of effects terminology to provide a common understanding of what the commander, planner, or targeting officer means when describing a particular effect for IO.

Service IO doctrine provides more guidance, but is little better. For example, Army doctrine lists eleven possible effects for IO categorized into offensive and defensive effects that range from traditional lethal effects such as "destroy" and "disrupt," to less definable nonlethal effects such as "detection" and "response."[1] For its part, Air Force doctrine lists nineteen possible strategic, operational, and tactical IO effects, including commonly used targeting effects (deny, degrade, disrupt, destroy), as well as other ill-defined terms such as "reduce," "hinder," "enhance," and "maintain."[2]

"Affecting an opponent's ability to use information is the focus for information operations, but it is not its purpose. IO's purpose is to use information to affect the opponent's decision-making and operations."

In the field, IO staffs are using dictionaries to find and define effects for IO. Left without clear doctrinal guidance, the planners are writing IO plans that include nebulous terms such as "promote," "inform," "preserve," and "mitigate."

The result is confusion. For IO planners and targeting officers, questions abound. What is an objective for IO? What are effects for IO? How do objectives differ from effects? This article discusses these questions and proposes a way of looking at objectives and effects in the information environment.

Conceptualizing Objectives for IO

According to Joint doctrine, an objective is:

1. The clearly defined, decisive, and attainable goals towards which every military operation should be directed.
2. The specific target of the action taken (for example, a definite terrain feature, the seizure or holding of which is essential to the commander's plan or, an enemy force or capability without regard to terrain features)."[3]

In its pamphlet, *Operational Implications of Effects-based Operations*, US Joint Forces Command, further explains that "At the theater-strategic levels, objectives focus more on the intended purpose of the operation, not just the military action. Rather than statements of action, these higher order objectives are expressed as operational or strategic goals, conditions, or outcomes, which describe the intended end-state from the combatant commander's perspective."[4] Extrapolating this view to information operations leads to the conclusion that an objective for IO is a statement of what the Joint force's information operation should achieve – a condition or outcome – in the information environment.

This realization questions what conditions and outcomes IO should create in the information environment. Before those outcomes can be identified, we need to understand the information environment and how organizations use it to support their operations. Using the domains of conflict model to analyze the information environment, we can conclude that at the most basic level, organizations use the information environment to collect, process, and disseminate information. Organizations perform these functions in order to facilitate decision-making, or to coordinate and execute physical actions.[5]

The broad objective of any force's operations in the information environment is to collect, process, and disseminate information better than one's opponent. Therefore, IO affects an adversary's ability to use information in order to give friendly forces an advantage in the information environment; i.e., an information advantage.[6] Once that is achieved, then one force can make decisions, and coordinate and execute physical actions better than its opponent.

A non-doctrinal term, information advantage means being in a superior position in the information environment relative to one's opponent. Specifically, an information advantage is sought and achieved in the information domain; that part of the information environment in which information exists and organizations collect, process, and disseminate that information.

Affecting an opponent's ability to use information is the focus for information operations, but it is not its purpose. IO's purpose is to use information to affect the opponent's decision-making and operations. In other words, the utility of an

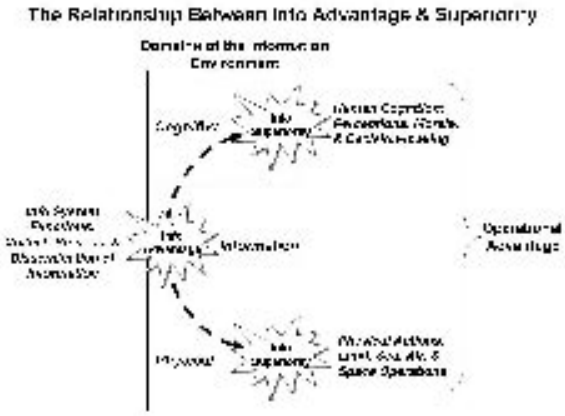
information advantage is that it generates effects that influence adversary and other organizations' decision-making, morale or perceptions in the cognitive domain and subsequent actions in the physical domain. In sum, these cognitive and physical effects create an operational advantage for the friendly force. For IO, this operational advantage is expressed as information superiority (see Figure 1).

Crafting IO Objectives

Restated from the preceding discussion, an IO objective is a statement of a specific condition or outcome in the information domain achieved through the use of information-related capabilities. If we are to use information as a military capability, then IO objectives must focus on the production of specific conditions in the information domain that in turn will contribute to information superiority. With this in mind, a useful format for an IO objective statement is: objective, target, function, and purpose.

Objective. An IO objective describes the specific condition resulting from attack (for lethal means) or engagement (for non-lethal means) of enemy or other's capabilities to operate in the information domain. Traditional targeting objectives are: *limit, disrupt, delay, divert,* and *destroy*.[7] Following this line of logic then, traditional objectives can be refined to fit the information domain by focusing on the information system functions of collect, process and disseminate:

- Limit. In conventional terms, limit "refers to reducing the options or courses of action available to the enemy commander. For example, a commander may want to limit enemy ability to use an avenue of approach or weapon system."[8] For IO, limit may mean to reduce the enemy's ability to operate in, or interact with, the information environment by restricting the enemy's options to collect and externally disseminate information.
- Disrupt. In the physical environment, disrupt "precludes the efficient interaction of enemy combat and combat service support systems. It forces the enemy into ineffective tactical dispositions and degrades movement of material, forces and supplies."[9] In the information environment, disrupt means to prevent the enemy from internally processing and distributing the information needed to accomplish its mission.
- Delay. During combat operations, delay means to "alter the time of arrival of enemy forces at a point on the battlefield or the ability of the enemy to project combat power from a point on the battlefield."[10] For IO, delay means to slow the internal processing and distribution of information used to support decision-making, or the ability to interact with others in the information environment.
- Divert. In conventional terms, divert "causes an enemy to tie-up critical resources so they can't be used at a point or time on the battlefield. Divert reduces the ability of the enemy commander to stay on plan or continue his mission."[11] For IO, divert causes the target to expend resources to collect, process, and distribute information that is useless to its mission needs.
- Destroy. To destroy is "to ruin the structure, organic existence, or condition of an enemy target that is essential to an



enemy capability."[12] For IO, this means to destroy enemy ability to perform the information system functions of collecting, processing, and disseminating information.

Traditional targeting objectives are inherently offensive in their approach and focused on enemy forces. As such, they do not adequately address defensive capabilities or address entities other than a declared enemy force. If planners are to adequately express all of IO's capabilities, as well as the use of the information environment to shape the area of operations, it is necessary to expand objectives for IO beyond just an application of the traditional objectives. With this in mind, other possible objectives for IO are:

- Deny. To withhold information about friendly force capabilities and intentions from adversary collection. For IO, this may mean preventing the collection of specific, critical information from enemy intelligence collection platforms.
- Preserve. To maintain the content and flow of information already present in the information environment. For IO, this means preventing the enemy from adversely affecting the information environment and the friendly force's ability to operate in the information environment.
- Exploit. To create or use information to alter the content and flow of information present in the information environment. This can mean highlighting specific events or actions in the operational area for the purpose of getting third parties to disseminate information to friendly force advantage.

Target. The target is what will be affected: an adversary formation or, depending on the mission, some other discrete individual, group, or organization in the area of operations such as a specific decision-maker, populace group or third party organization that is critical to enemy or friendly forces or can threaten mission accomplishment.

Function. An IO objective should also address a specific information system function of the target. More specifically, an objective should address how it will affect information collection, processing, or dissemination (both internal and external). By affecting the function, IO objectives are focused on the means by which an organization, military or civilian, makes use of and affects information content and flow in the information environment.

Purpose. The purpose of an objective focuses the information operation on achieving information superiority. As such, it should clearly identify the specific operational

advantage (as opposed to information advantage) sought. To craft the purpose of an objective, it is necessary to discuss how IO creates effects in the physical and cognitive domains.

Effects in the Information Environment

While objectives for IO express a condition or outcome in the information domain, an effect for IO must express a condition or outcome in the real world – that is, the cognitive or the physical domains. Unfortunately, there is no definitive doctrinal list of effects, or for that matter, even a doctrinal definition of "effect."

In lieu of a doctrine, the US Joint Forces Command definition must suffice. An effect is "the physical and/or behavioral state of a political, military economic, social, infrastructure, information system that results from a military or nonmilitary action or set of actions."[13] An "effect" describes a desired state in the cognitive or physical domains. For IO, these effects are generally manifested as conditions affecting either the target's information systems in the physical domain, decision-making in the cognitive domain, or subsequent behavior in the physical domain.

Cognitive Effects. Effects in the cognitive domain should describe a psychological condition or state that will manifest itself in the mind of the target. While non-specific terms like "influence" are used liberally throughout the IO community, more discrete effects are required to convey the true purpose of IO.[14] Possible cognitive effects are:

- Mislead. A target is misled when it believes something that is not true. This specific effect should be used when the commander desires to drive the adversary to make a specific decision or form a specific perception.
- Confuse. A target is confused when it does not know whether or not to believe something is true. This effect is used when the commander desires that the adversary cannot make an informed decision due to poor information.
- Degrade. The term degrade is often used to describe a physical effect, but it also has applicability in the cognitive domain. In this sense, degrade is to reduce adversary or third party morale, perceptions, or attitudes. For example: degrading popular support for a particular insurgent group.
- Promote. Just as a force may want to degrade perceptions and attitudes, it may be desirable to promote specific perceptions and attitudes. Promote then, can be to increase support for, or to awareness of the friendly force presence and activities.
- Inform. To increase target audience situational awareness and knowledge with out seeking to change perceptions and attitudes. Inform could be a preparatory condition prior to seeking a change in the target's cognition.

Physical Effects. Effects in the physical domain should describe a physical, behavioral condition or outcome exhibited by the target. For IO, information systems and networks (both technological and human) are attacked or engaged to generate physical effects. Possible physical effects can be numerous. A sample is:

- Destroy. A familiar term to conventional operations, destroy is applicable to describe effects in the information environment as well. As an effect for IO, destroy is to physically render adversary information systems useless or ineffective unless reconstituted.
- Degrade. In the physical domain, degrade means to physically reduce the effectiveness or efficiency of adversary employment of combat power. For IO, affecting the collection, processing, and dissemination of information can degrade the enemy's ability to synchronize and execute operations.
- Protect. Physical protection is a defensive condition to mitigate the effects of adversary actions in the information environment on friendly force information systems. Stated a different way, IO will affect how the adversary collects, processes and disseminates information in order to protect friendly capabilities from physical attack.
- Isolate. To physically separate the target from the information needed for situational awareness and decision making.

Putting it All Together

When objectives and effects are put together using the format described above, IO objectives can be written as follows:

- Cognitive Example: Limit 34th Armor Division collection of pre-operational movements in order to mislead the enemy commander of the time and place of the attack.

Objective:	Limit
Target:	34th Armor Division
Function:	Collection of pre-operational movements
Purpose:	Mislead the enemy of the time and place of the attack

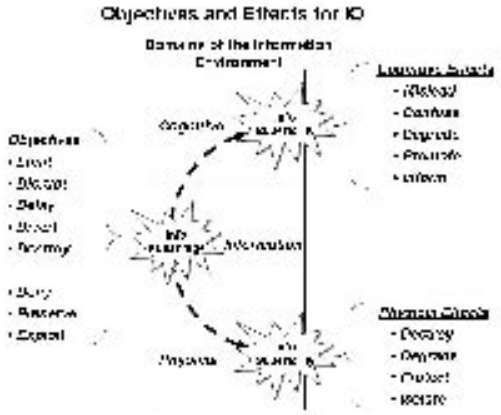
- Physical Example: Disrupt leader X's dissemination of anti-government propaganda in order to degrade the size of violent anti-government demonstrations.

Objective:	Disrupt
Target:	Leader X
Function:	Dissemination of anti-government propaganda
Purpose:	Degrade the size of violent anti-government demonstrations

Using this technique, an IO objective is able to communicate two important points. First, it shows how IO will affect the collection, processing, and dissemination of information in order to generate an operational advantage. Second, it communicates a discrete effect that is easier to assess than the sweeping and imprecise effects typically written into IO plans.

It should be reiterated that there is a significant difference between IO objectives and effects. Objectives for IO describe a condition in the information domain, while effects describe a desired state in the cognitive or physical domains resulting from an information advantage (see Figure 2).

Conclusion



Clearly, if the Joint Force is going to harness the power of information and convert it into a warfighting capability, it is necessary to change how IO objectives and effects are currently expressed. Admittedly, the concept presented in this article requires testing and validation in the field. Objective and effects terminology are by no means definitive. Rather, it is hoped that the practitioners of IO will adopt some of the ideas in this article and be able to refine and improve how IO as a discipline can more clearly and articulately express how it contributes to modern military operations.

Endnotes

[1] US Army Field Manual (FM) 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, November 2003, pages 1-16 and 1-17. Offensive effects are: destroy, disrupt, degrade, deny, deceive, exploit, influence. Defensive effects are: protection, detection, restoration, and response.

[2] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005, pages 29-31. Strategic effects include: influence, reduce, and deter. Operational effects include: hinder, slow, reduce, influence, enhance, disrupt, and protect. Tactical effects include: deny, degrade, disrupt, deceive, destroy, reduce, influence, protect, and maintain.

[3] Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*.

[4] US Joint Forces Command (USJFCOM) Joint Warfighting Center (JWFC) pamphlet, *Operational Implications of Effects-based Operations (EBO)*, page 12.

[5] For a detailed discussion of see "A Theory-Based View of IO" by Marc Romanych (*IO Sphere*, Spring 2005), pages 12-16. In brief, the physical domain is the tangible portion of the information environment where information systems and networks exist and are employed. The information domain is an abstract space created by the intersection of the physical and cognitive domains. This is the domain through which communication takes place and is where the functions of physical information systems occur (i.e., information collection, processing, and dissemination). This is also the domain where information resides. The cognitive domain is the individual and collective consciousness of human beings and consists of those elements of human thought that influence decision-making and behavior.

[6] The definition of information advantage is from CCRP's work *Understanding Information Age Warfare* by David S. Alberts., John J. Garstka, Richard E. Hayes, and David A. Signori (DoD Command and Control Research Program, Washington D.C., 2001), pages 54-57.

[7] These terms are used by the Army and Marine Corps to describe the effects of attack on enemy capabilities. While some of these terms are also Joint interdiction objectives, no other Service has an analogous list of terms. Therefore, these terms must suffice to establish a basis for discussion. While the Army and Marine Corps also use the term *damage* as a targeting objective, it is generally associated with nuclear objectives and is identified as undefined and subjective.

[8] US Army FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, May 1996, page 1-2.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] US Joint Forces Command (USJFCOM) Joint Warfighting Pamphlet 7, *The Operational Implications of Effects-based Operations*, page 11.

[14] Influence is a commonly used effect for IO; however, it is vague and unquantifiable as a description of a psychological condition or state.