Measures of Effectiveness in the Information Environment

By Lieutenant Colonel David C. Grohoski, Steven M. Seybert (Major, USA Retired), and Marc J. Romanych (Major, USA Retired)

Assessing the effectiveness of an information operation is one of the greatest challenges facing a staff. Despite the evolution of information operations (IO) doctrine and the refinement of supporting tactics, techniques, and procedures (TTP), the problem of IO assessment methodology is still unsolved. The question remains: lacking physical evidence, how does an IO staff quantify the intangible attributes of the information environment in order to assess the effectiveness of the information operation?

This article addresses the matter of quantifying an information operation's effectiveness and presents a methodology for developing measures of effectiveness (MOE) to ascertain IO effects on friendly and enemy forces.

Statement of the Problem

Why is assessing the impact of an information operation so difficult? First, the information environment is an abstract construct and IO operates within that construct. According to Joint Publication 3-13, *Information Operations*, the information environment is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information. Also included in the information environment is information itself. Thus, the information environment is a combination of physical assets (e.g., information systems) and non-physical concepts (e.g., information, information-based processes, and human decision making processes). IO attacks and protects the physical assets of information systems in order to affect the non-physical aspects of the information environment. Transitioning from visible effects resulting from destruction of tangible assets such as command posts and radar systems to abstract effects such as disrupted information flow and degraded decision-making is a challenging task.

Second, not all of IO's capabilities reside in the physical world. While physical destruction is tangible enough, many capabilities are non-physical – operations security (OPSEC), electronic warfare (EW), military deception, psychological operations (PSYOP), etc. The effects ultimately produced by these elements are intended to occur in the intangible domain of ideas, perceptions, and attitudes. Capturing data or information to measure such non-physical effects is difficult and often time-consuming, requiring a depth of analysis that seems impossible during high-tempo operations.

Third, an integrated information operation achieves a complex, tiered hierarchy of effects (Figure 1). The attack or protection of physical assets (information systems) yields what can be called first-order effects, such as the destruction, degradation, and disruption of enemy signal nodes and command posts, or perhaps the presentation of false observables for collection by enemy intelligence systems. These first-order

activities are directed against the enemy's information system to achieve second-order effects on the enemy's information and information-based processes, which in turn, seek a third-order effect on the enemy commander's decision-making (i.e., the ultimate target of IO). Defensively, first-order effects may be the protection of friendly force information system assets, second-order effects may be the maintenance of situation awareness or an uninterrupted information flow, and third-order effects may be the preservation of effective decision-making. Each level of effects will, in all likelihood, yield corresponding enemy and friendly reactions, resulting in a complex, tiered set of cause and effects, which must be identified and interpreted if the overall impact of the information operation is to be determined. To sort through this maze of causal relationships, something more than traditional battle damage assessments (BDA) is required.

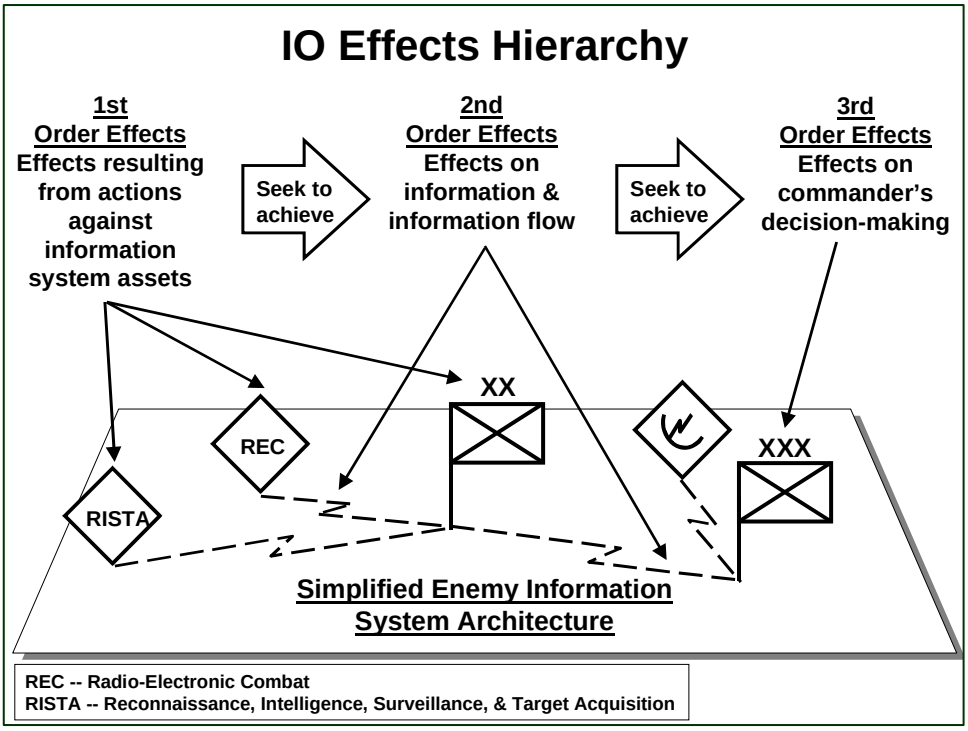

Figure 1

Assessment and the Hierarchy of Effects

IO assessment is the determination of the overall effectiveness of the information operation. Measurement and analysis of effects resulting from the attack of enemy information systems and protection of friendly information systems make such an assessment possible. However, to do this, it is necessary to understand the hierarchy of effects resulting from IO activities (e.g., first-, second-, third-order effects).

First-order effects result from those actions directed against the enemy's information system and taken to protect the friendly information system. Generally, first-order

effects are deduced by using information derived from unit reporting and BDA.[1] This level of assessment determines if planned offensive and defensive IO tasks have occurred and the direct result of these actions and activities. Second and third-order effects are those generated by the sum total of actions directed against enemy and friendly information systems. These effects are less detectable and quantifiable than first-order effects. At these levels, assessment seeks to determine if the aggregate of executed IO tasks have achieved the desired result – what were the effects on the enemy and friendly information systems (second-order effects), were the enemy and friendly commanders affected (third-order effects), and if so, how and to what extent? Second and third-order effects are usually determined through inductive analysis of intelligence reporting and assessments.

Establishing Cause and Effect

Because IO and the information environment are a mixture of physical assets and abstract concepts, the only way to achieve cause and effect linkages is to acknowledge that military conflict consists of interactions between humans and technology. Also, it is assumed that the physical assets of a military force and the intangible aspects of military operations, such as morale, leadership, will, and cohesion, are linked. Thus, attacking physical assets – command posts, target acquisition systems, intelligence collection and processing systems, and communication systems – will adversely impact a military force's ability to make and act upon decisions and consequently will have a detrimental affect on those intangibles that provide the military force with the ability to conduct operations.

Establishing a linkage, or correlation, is necessary to determine whether IO actions and activities are impacting friendly and enemy information flow and decision-makers. Correlation exists when the value of an action (e.g., number of occurrences, degree of the effect, etc.) increases (or decreases) while the value of the effect also increases (or decreases). For example, if as the number of PSYOP leaflets dropped on enemy formations increases so do the number of enemy soldiers surrendering, or if as the number of jamming attacks against a command and control net increases, the traffic on that net decrease; then correlation exists. This deductive reasoning forms the basis of determining first-order effects.

However, the relationship between action (cause) and effects may be coincidental, meaning that the occurrence of an effect is either purely accidental or perhaps caused by the correlation of two or more actions executed to achieve the effect. For example, if friendly forces are successfully engaging enemy formations with fire and maneuver at the same time PSYOP activities are urging enemy soldiers to surrender, then correlating an increase in surrendering soldiers to PSYOP activities may not be possible. Furthermore, because an information operation will often employ multiple

[1] Unit reporting and BDA address the success or failure of planned IO tasks to attack enemy and defend friendly information system assets. This information helps determine which enemy and friendly assets are affected and yields an estimate of the immediate results. The purpose of this first-order assessment is to determine if current IO tasks and the level of effort applied to the information operation are adequate.

elements to engage the enemy's information system, the cumulative effect of IO support to friendly combat actions may make the impact of individual IO activities indistinguishable. Since there will rarely be enough time to definitively rule out coincidental relationships, the only possible antidote is an in-depth knowledge of the enemy and information environment that facilitates the development of an informed estimate through inductive reasoning.

What are Measures of Effectiveness?

Unfortunately at the present time, no doctrinal definition of MOE exists. For this discussion, the following definition is proposed – measures of effectiveness are standards of reference used as bases of comparison to evaluate the success or progress of an operation.

MOE are a means to determine second and third-order effects by establishing a cause and effect linkage between the usually observable and quantifiable first-order effects and the abstract and subjective second and third-order effects. MOE do not constitute the assessment itself, but are an evaluation means to determine if the individual IO tasks are achieving the IO objectives and whether accomplishment of the IO objectives is fulfilling the concept of IO support (Figure 2).[2]

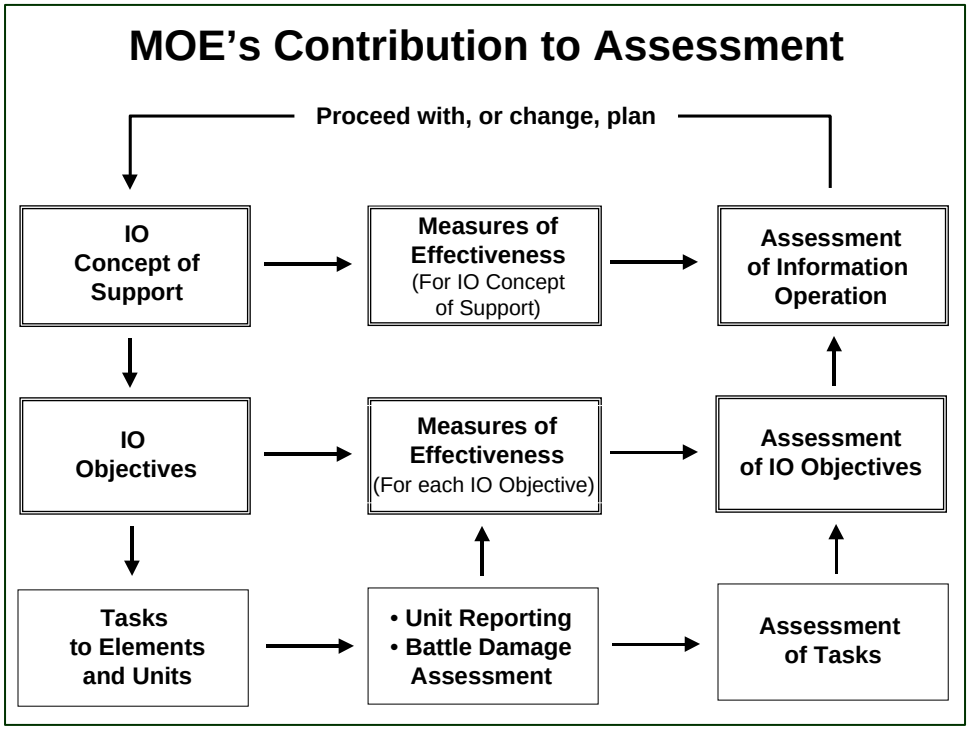

Figure 2

[2] MOE may be developed to measure the accomplishment of individual IO tasks. Doing so is largely dependent upon the importance of the task, as well as the availability of resources and time to plan and conduct an assessment to that level of detail.

Developing MOE

MOE are developed as part of the planning process to determine the effects of both offensive and defensive IO. To be meaningful, MOE must link friendly and enemy actions and activities (cause) to enemy and friendly capabilities to make and act upon decisions (effect).[3] Therefore, MOE development begins with the IO concept statement and objectives.[4]

If the IO concept statement and objectives are not properly crafted, then developing corresponding MOE will be difficult, if not impossible. The IO concept statement identifies succinctly what the information operation must do to support the command's mission successfully. Therefore, the IO concept statement should be focused on specific aspects of the operation and not be so general that it merely identifies standard doctrinal requirements for IO. An example of a simplified operational-level IO concept statement is: On order, Joint Task Force (JTF) 451 conducts information operations in the Joint operations area in order to disrupt Northland command and control and influence local leaders and populace, allowing the destruction of Northland armed forces.

MOE are developed to assess each IO objective's desired effect.[5] Ideally, each objective has a clearly defined, attainable effect, otherwise it is not possible to determine if, or when, that effect is achieved, and hence, whether the IO objective, is met.[6] Example IO objectives for the previous IO concept statement are:

- Disrupt Northland air defense forces' capability to integrate early warning and acquisition systems.
- Neutralize Northland reconnaissance assets' ability to detect the JTF's main offensive effort.

---

[3] William S. Murray, "A Will to Measure," *Parameters*, (Autumn 2001), p 135.

[4] The IO concept, often called the IO mission statement, is a statement of what IO is expected to do in support of the command's mission. Although by doctrine, a mission statement is included in each annex to a plan, the author's believe that there should only be one unit mission statement per operation. Therefore, in this article the "IO mission statement" is referred to as the "IO concept statement".

[5] A well-crafted IO objective specifies an effect, an object of the effect, and a purpose for the effect. Normally, offensive IO objectives are written in terms of causing an adversary to do or not do something. Defensive IO objectives are written in terms of protecting and defending friendly force's information and information systems.

[6] It is important to note that doctrine does not provide specific effects for IO. Typical effects used in the field are: deny, destroy, degrade, disrupt, deceive, exploit, and influence. Some of these effects are taken from targeting and therefore have specific definitions, while other effects are simply used because they seem appropriate to IO. Having well defined effects will certainly assist the planning and development of IO objectives and MOE. Another noteworthy aspect of IO doctrine is the lack of terms for describing defensive IO effects.

- Disrupt Northland ground force commander's synchronization of corps and army-level operations.
- Influence local civilian leaders and population groups to not interfere with JTF forces and operations.

As previously noted, MOE for second-order effects seek to determine if the aggregate of IO actions and activities are accomplishing the IO objectives. If ***possible***, the MOE should be observable to aid intelligence collection, quantifiable to increase objectivity, precise to ensure accuracy, and correlated to the progress of the operation to attain timeliness. While it is possible for an IO objective to have multiple MOE, bear in mind that intelligence collection and analysis assets are limited. Possible second-order MOE could be:

- Ninety percent or more of Northland early warning sites and air defense sector control centers suppressed.
- No JTF air attacks are effectively engaged by radar-guided SAMs.
- No JTF high-value assets are attacked by surface-to-surface fires, air strikes, or special purpose forces' direct action.
- Northland 1st and 2nd echelon ground forces are unable to synchronize fires and maneuver above division level.
- Northland strategic reserve forces are not committed against the JTF's main ground attack before penetrating the second operational echelon.
- No JTF main supply routes are blocked by the civilian populace.
- No instances of local leaders inciting the populace to interfere with JTF operations.

MOE for third-order effects seek to determine if the enemy and friendly commanders were affected as planned by the information operation. These MOE should determine if the decision-maker has responded as predicted. Thus, in all likelihood these MOE will be subjective. Possible MOE for third-order effects may be: Northland commander unable to block or counter-attack the JTF's main offensive.[7]

Figure 3 provides an example of an IO concept, objectives, and supporting MOE.

[7] This MOE assumes that the enemy commander's predicted decision (as determined by the J2's IPB), was to either block or counter attack the JTF's ground offensive.

Example IO Objectives and MOE

IO Objective	1st Order MOE (BDA)	2nd Order MOE	3rd Order MOE
Disrupt Northland ground force commander's synchronization of corps and army-level operations.	• **Destruction of corps & army headquarters.** • **Destroyed or captured reconnaissance teams** • **Decreased corps-level and above command & control commo traffic.** • **Increased division command & control net commo traffic.**	• **Northland 1st and 2nd echelon ground forces are unable to synchronize fires and maneuver above division level.** • **Northland strategic reserve forces are not committed against the JTF's main ground attack before penetrating the second operational echelon.**	**Northland commander unable to block or counter-attack the JTF's main offensive.**

Figure 3

Assessment – Putting it all Together

MOE are but one part of the assessment process. Traditional BDA and other intelligence analyses, as well as friendly unit reporting, are still key to assessing the information operation's effectiveness. These sources provide the information on quantifiable effects that can be used as the basis for estimates of whether the IO objectives and concept of IO support are being achieved. As previously noted, information derived from unit reporting and BDA are typical sources for determining first-order effects, while intelligence reporting and assessments provide the information to determine second and third-order effects.

Once MOE are written, then a mechanism to obtain the information needed to determine the three orders of effects is developed. The IO staff must determine: the assessments that must be made, the specific information needed to make the assessments possible, and the agencies and assets that will provide the information. This assessment plan then contributes to the command's intelligence collection plan and Friendly Forces' Information Requirements (FFIR).

Timely and accurate reporting of information is essential to assessing effectiveness of the information operation. Much of this information is reported from subordinate units to higher headquarters. Maneuver units, tactical PSYOP teams, and civil affairs tactical support teams, as well as tactical human intelligence (HUMINT) teams and other intelligence collection assets all provide information with which to gauge IO's success. Additionally, on-going intelligence analysis, including analysis of media and other open

sources, supports assessing whether IO is achieving its objectives and if the IO concept of support is successful.

To receive information, the IO staff must actively monitor the operational situation and aggressively pursue information through unit reports and debriefings, IO working group (IOWG) meetings, and other venues. Commanders' battle update briefings, conference calls, and other meetings also facilitate monitoring IO execution by providing a forum from which information is received for subsequent analysis. Some other actions the IO staff can do are:

- Submit Requests for Information (RFIs) based upon the assessment plan.
- Develop IO input to the Commander's Critical Information Requirements (CCIR).
- Coordinate with the Deep Operations Coordination Cell (DOCC) and targeting board for BDA reporting.
- Review assessments at each IOWG.
- Monitor J2 and J3 incident databases and analyze trends.

Ultimately, an assessment is successful when it is possible to decide when to proceed with the plan, when to re-engage a target, when to execute a branch of the plan, or when to execute a sequel.[8] MOE fit into this effort by facilitating the organization and assessment of the information needed to support these decisions.

Conclusion/Summary

Developing MOE to assess the effectiveness of the information operation is a difficult task. In many respects, MOE is much more art than science. However, through development of proper MOE and an effective assessment plan as discussed in this article, then the science involved in achieving and assessing first-order effects can be linked to the more subjective assessments of accomplishing second and third-order effects. Thus, an informed estimate of the effects resulting from execution of a command's IO tasks can be made and the progress of the information operation established.

Clearly more work has yet to be done. However, as IO practitioners continue to work with MOE and other assessment methodologies, they will refine and validate successful techniques and procedures.

[8] By U.S. Army definition, a branch is a contingency plan or course of action for changing the mission, disposition, orientation, or direction of movement of the force to aid success of the current operation based on anticipated events, opportunities, or disruptions caused by enemy action. Sequels are future operations that anticipate possible outcomes – success, failure, or stalemate of the current operation.

Authors' Biographies

Lieutenant Colonel David C. Grohoski is currently the Chief of the U.S. Army Land Information Warfare Activity (LIWA) Field Support Division. A career infantry officer, his previous assignments include Battalion Senior Observer/Controller at the Joint Readiness Training Center (JRTC), Exchange Officer in the British Army, Executive Officer of The Old Guard, as well as assignments in light infantry and airborne ranger units. He is a Distinguished Military Graduate of Michigan State University and received a Masters Degree from the University of Oklahoma.

Major Steven M. Seybert, U.S. Army (Retired), works for Coleman Research Corporation and has provided contract support to the U.S. Army Land Information Warfare Activity (LIWA) for over four years of planning and conducting information operations (IO). He has planned and executed IO with LIWA field support teams (FSTs) on more than 25 deployments to various levels of military command from joint task force to division. He performed as the IO targeting officer while deployed with a LIWA FST to the Multi-National Brigade – East in Kosovo from March to August 2000. He is a graduate of the U.S. Military Academy at West Point and the Command and General Staff Course. He can be reached via e-mail at smseybe@liwa.belvoir.army.mil or steve.seybert@us.army.mil.

Major Marc J. Romanych (U.S. Army Retired) is a former Air Defense Artillery Officer. He works for JB Management Inc., contracted to the U.S. Army Land Information Warfare Activity (LIWA). Since 1998, he has deployed with LIWA information operations field support teams to Bosnia and on numerous Joint and Army warfighter exercises. He holds degrees in Chemistry, Geology, History, and International Relations. Readers may contact him via e-mail at mjroman@ liwa.belvoir.army.mil or mjromanych@cs.com.