IO Measures of Effectiveness

By Mr. William R. Swart, Senior Executive Service-4

Editorial Abstract: *Measures of effectiveness are key to assessing joint operations. The complex nature of many information operations capabilities often makes assessment even more challenging. In this article, Mr. William Swart, JIOC Technical Director, proposes that concepts originating within the DOD C4I community can be used to advance the development of IO measures of effectiveness.*

Throughout the evolution of information warfare (IW) and information operations (IO), I've heard more times than I can count statements similar to: "What IO really needs to become a success are Measures of Effectiveness (MOE)". I stopped to think about this statement and offer, in this article, a few ideas on the topic.

First of all, MOE for IO is a very complicated subject because the scope of IO is very broad and all encompassing. The DoD definition of IO states IO are those "actions taken to affect adversary information and information systems while defending one's own information and information systems.[1]" To over simplify the definition, this means both information and information systems can be and are the targets of IO. Where it may be possible to quantitatively measure effects on information systems, it is extremely troublesome to measure effects on information. This is because information has an indeterminate value without defining its use and its context.

I believe there are valuable concepts that originate within the DoD C4I community that can be borrowed to advance the development of IO MOE. The concept of information architectures as extracted from the DoD C4ISR Architecture Framework[2] can be used to help identify and define MOEs for IO. A C4I architecture description is analogous to a blueprint that describes all the components of a network, what the components do, how they relate and the rules that govern their functioning. There are three fundamental perspectives in an overall information architecture. They are the operational view, the systems view and the technical view. Figure 1 provides a graphical depiction of these views and their interrelationships.

The operational view is a description of tasks, activities, functions, processes and associated information flows necessary to make operating decisions. The systems view is a description of the links and nodes in a networked environment that implement the operational perspective by associating physical entities and their associated characteristics and performance with the operational view and its requirements. The systems view is linked to the operational view by 'Information Exchange Requirements'. The technical perspective is the set of rules governing the performance and interaction of the systems components including all conventions, criteria, parameters and standards applicable to the implementation of the network.[3]

The definition of 'measures of effectiveness' must be derived from the definition of 'effects'. A relevant definition of effects in a military context was found in Air Force Doctrine publications. "Effects are physical and/or psychological outcomes, events or consequences that result from a specific military action.[4]" This defines the highest echelon of result and in DoD acquisition-testing terminology is best referred to as measures of operational outcome (MOO). At this echelon, MOO will normally require measures of human decision behavior and will involve mostly qualitative judgements. At the technical level, the measures of performance

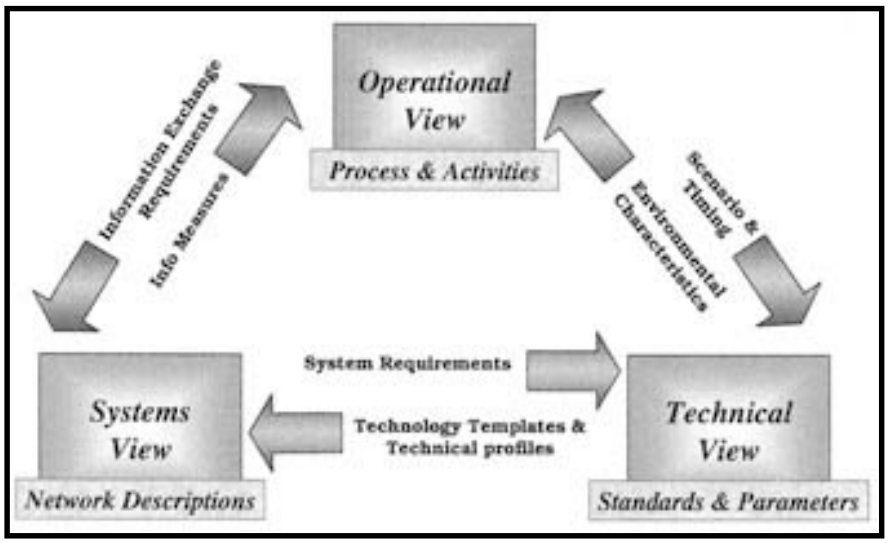

Figure 1 Information Architectures

Use/ Destination			Source		Communications Mode		Attributes		
Nodes	Activity Supported	Element of info	Producing Node	System	Media	Format	Units	Accuracy	Timeliness
1	Air Defend	A/C Track	Reporting Post	TPS-M Radar	Mircro-wave Radio	ASCI Text	LAT/ Long	500M	10 Sec
2	C2								
3									
4									
.									
.									
.									
.									
.									
.									
N									

Figure 2: Information Exchange Matrix

(MOP) are very quantitative and include metrics such as capacity, speed, through-put, jam to signal ratio, bits per second, bit error rate, etc.

At the systems level, measures of effectiveness need to and can be defined. This is the remaining focus of attention for this paper. The key to defining MOE at the systems level is the information exchange requirement. It defines the informational context upon which the military activities of attack and defense can be evaluated. Figure 2 depicts a hypothetical matrix describing the information exchange requirements linking a systems architecture description to its associated operational architecture description.

Since effects are the result of action or cause, it is useful to think first of the IO actions that can impact the flow of information and hence affect the functioning of an operational architecture. Potential military IO actions include destroying, disrupting, or degrading, which is done against information systems. Other actions such as denying or delaying are targeted against the information itself. Finally deceiving (misleading), influencing or informing are actions involving information content that are focused on the ultimate use of information, most normally the human decision-maker. Conceptually these actions can affect the flow of information in four fundamental ways. The first result may be to reduce the quantity of information or sources of information available for the using nodes. Second may be to make the elements of required information partially or totally incomplete. Third may be to degrade or modify the accuracy of the information. Finally the information might be delayed. Therefore it is proposed that four fundamental MOE for IO are quantity, completeness, accuracy and timeliness. These metrics evaluated against the specific information exchange requirements can be expressed in terms of either absolute values or percentages. These values should offer the Joint Force commander the opportunity to quantitatively evaluate and compare alternative course of action.

In summary, it is believed that MOE can be developed and applied to IO. It is proposed that the DoD C4I community has already provided a useful conceptual framework for defining these MOEs. The remaining challenge, which, most important at the operational level of command, is to answer the "so what" question and define Measures of Operational Outcome. That challenge is left to another day.

References:

[1] DoD Directive S-3600.1 "Information Operations", 9 December 1996, p. 1-1.

[2] C4ISR Architecture Framework; Version 2.0; 18 December 1997

[3] C4I Support Plan Guidance & Format; Version 1.2; December 1999, Internet, http://classic.deskbook.osd.mil/valhtml/2/24/242/242T03.htm

[4] Draft Air Force Doctrine Document 2-1.2; Strategic Attack, 1 March 2001, Internet, https://www.doctrine.af.mil/Main.asp?Set=0

Mr. William R. Swart, a member of the S Executive Service, is the Technical Director of the J Information Operations Center (JIOC), Lacklan Air Force Base, Texas. In this position he is th principal scientific and technical advisor to the Commander of the JIOC and is responsible for planning, coordinating, and executing the technical and engineering policies and programs of the JIOC. He has held this position since December 1987 Mr. Swart's career includes various electroni engineering assignments dealing with the research a development of advanced long-range radar systems, p array antennas, advanced signal processing, and new command, control, and communications countermeasures systems.

Mr. Swart is a graduate of Union College, Schenectady, NY, earning a Bachelor of Science degree in Physics in 1968. He holds a Masters of Science Degree in Systems Management from the University of Southern California. He completed the program in Executive Excellence at the Federal Executive Institute in 1988 and Harvard University's programs for Senior Executives in National and International Security in 1990 and Senior Managers in Government in 1994.