

---

## SUMMARY

---

The primary objective of this work is to create a framework for developing measures and metrics that adequately assess the impact of varying command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems and procedures on combat outcomes. In the process, sample measures and metrics are suggested to achieve this goal.

Although measures are simply *bases* or *standards* of comparison and can therefore be described qualitatively, metrics must be mathematical expressions that allow us to evaluate not only the relative effect of alternative C4ISR systems on combat outcomes but also the degree to which one is better or worse than another. This argues for strict mathematical formulations that produce accurate results. It is important to note, however, that the process reported in this document is deductive—i.e., none of the equations presented in the text was based on experimental or operational data. Verification, validation, and calibration remains a task for future work.

The framework and the measures and metrics developed are demonstrated using a spreadsheet model based on techniques including graph and complexity theory, reliability theory, search theory, information entropy theory, and queuing theory. The objective is to demonstrate a proof-of-concept tool that can quickly generate several alternatives based on varying operating procedures, network connectivity, and C4ISR systems.

## BACKGROUND

Traditional measures of effectiveness (MOEs) usually ignore the effects of information and decisionmaking on combat outcomes. In the past, C4ISR operations have been analyzed separately using measures of performance (MOPs). The effects of changes in C4ISR operations on combat outcomes have been inferred rather than directly assessed, and therefore the quantifiable link between variations in C4ISR capabilities and combat outcomes has been relatively difficult to assess.

Add to this the assertion that a richly connected network of C4ISR facilities and weapon systems will improve decisionmaking and therefore favorably impact combat operations and the assessment problem becomes even more complicated. This latter idea is embodied in the concept of network-centric warfare (NCW).

### Network-Centric Warfare

Network-centric warfare is generally thought to be *the linking of platforms into one, shared awareness network in order to obtain information superiority, get inside the opponent's decision cycle, and end conflict quickly*. In contrast to network-centric operations or warfare, traditional warfare is considered to be *platform-centric*. The difference between the two is that in platform-centric warfare, one must mass force to mass combat effectiveness because each weapon system acts independently, whereas in network-centric warfare effects are massed, rather than force. That is, weapon system employment is “optimized” to improve aggregate performance, possibly at the expense of individual unit performance.

### The Framework

The framework adopted in this report uses graph theory to assess the value or cost of connectivity and information theory to assess the value of collaboration in the context of simple operational models.

Graph theory can be used to represent the flow of data and information in naval warfare. It can be used to differentiate full participants in decisionmaking from outside monitoring. It can also be used to represent the complexity of data or information flow in decision pro-

cesses. Once data and information pathways have been established, the decisions to be supported are determined and decision rules are developed.

Information theory is used to assess the “amount” of knowledge available in a command and control system. To do this, we apply the concepts embodied in information entropy or Shannon entropy. Where uncertainty exists, information entropy can be assessed—provided the uncertainty can be expressed as a probability. In general, entropy measures the amount of information available in the distribution. We use this to make the intellectual leap to measuring the knowledge level about the uncertain random variable. The additional information made available by collaboration increases the reliability of situation assessments, so reliability theory is a useful tool for studying collaboration. In the Time-Critical Target (TCT) vignette, we demonstrate how a priori knowledge (in this case of target behavior) can be combined with knowledge gained through collaboration. In the same vignette, we also demonstrate how knowledge improvements can be quantified in a way meaningful to operators.

Command and control alternatives, such as Cooperative Engagement Capability (CEC), are evaluated in this paper using simple sensor and weapon models to demonstrate the feasibility of analyzing the benefits of any improved information and the cost of possible information overload.

### **Analysis Implications for NCW**

NCW is not just about networks. Networks are necessary but are not a sufficient ingredient to effective network-centric operations, and performance may or may not improve significantly with increases in network size. Instances may occur in which burdens of network complexity outweigh gains of increased opportunity to collaborate.

In addition, collaboration is generally, but not always, beneficial. Among the factors that affect the value of collaboration is the knowledge the decisionmaking team members possess about the critical element(s) of the operation and their level of experience in acting as a team. A team capable of highly effective collaboration is not apt to benefit appreciably from additional members—regardless of the new members’ knowledge.

### THE SCENARIO

The conflict hypothesized involves a small island country facing a large hostile neighboring nation determined to annex the island. The fact that the primary attack routes are over water, along with the small island country’s dependence on sea lines of communication (SLOCs) and air lines of communication (ALOCs), implies a significant naval component. Setting the conflict 10 years into the future provides time to implement emerging NCW concepts as well as some new Navy systems.

The island’s strategic objective is to “hold on” against an anticipated massive enemy application of force early on. The enemy hopes that this will force an early capitulation. At a minimum, the island nation must hold out until the U.S. intervenes. Figure S.1 illustrates the situation as the island prepares to defend against an anticipated attack.

U.S. forces are positioned to assist the island improve its defensive posture against enemy missile attacks. Two carrier battle groups (CVBGs) will be positioned east of the island. Cruisers and destroyers will screen the carriers with additional cruisers assigned ballistic

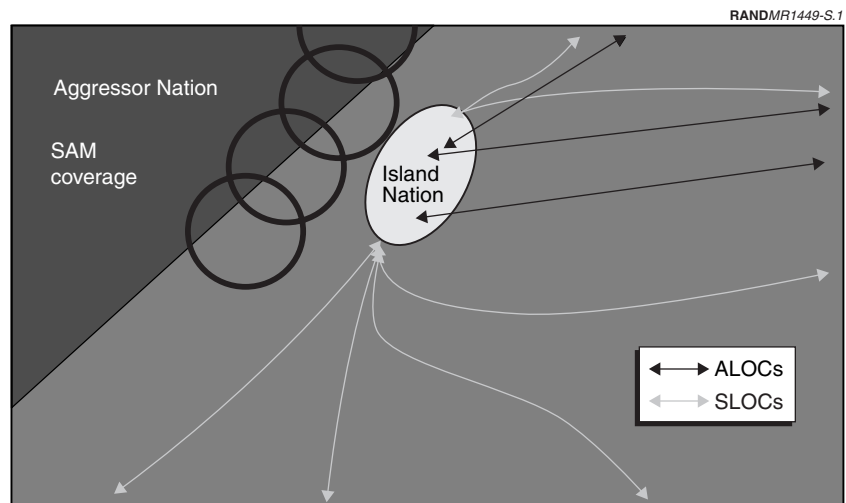


Figure S.1—Theater of Operations

missile defense duty off the island's two main ports. Nuclear-powered attack submarines (SSNs) will be assigned antisubmarine warfare responsibilities against enemy interdiction submarines.

## **CRUISE MISSILE AND BALLISTIC MISSILE DEFENSE**

This first vignette examines the information aspects of ship defense against antiship cruise missiles (ASCM) while those ships conduct theater ballistic missile defense (TBMD). Once launched, cruise missiles and ballistic missiles enter an initial engagement queue. If no interceptor missile defeats the incoming attack missiles, one of two things will occur: ASCM leakers will join a second queue to be "serviced" by the Close-In Weapon System (CIWS) on board the cruisers or ballistic missile damage to land targets will be assessed.

Two pairs of Aegis cruisers are assigned to cover an area of operations to defend against enemy cruise and ballistic missile attack. Given their role in defending friendly territory, the cruisers themselves are also likely to be targets, and therefore they are prepared to defend against such an attack.

### **Measures of Performance and Force Effectiveness**

The Aegis cruisers have two (competing) missions: prevent enemy ballistic missiles from destroying key allied infrastructure targets and defend against cruise missile attacks. For both missions, the obvious measure of success is survivability—that is, *the fraction of the critical infrastructure targets that survive the attack and the "fraction" of the cruisers that survive the attack.*

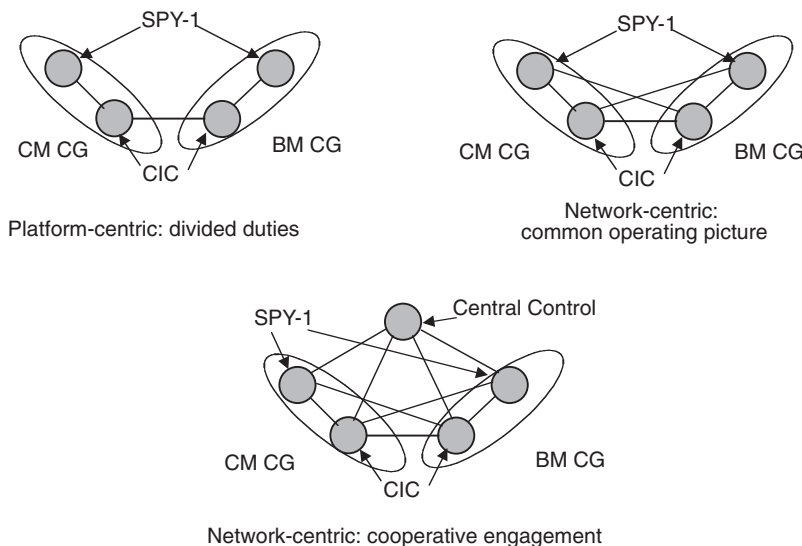
What is not known is the attack distribution for ballistic missiles and cruise missiles—i.e., how the enemy will schedule the attack to ensure that the friendly infrastructure targets are destroyed while at the same time minimizing interference from the defending cruisers. For purposes of this analysis, all other factors are known. The MOP therefore is *the degree to which the friendly commander "knows" the enemy's attack distribution.* Knowing the attack distribution contributes directly to the allocation of interceptors and therefore to the effective defense of both the cruisers and the friendly infrastructure targets.

### Alternatives

Aegis cruiser radars cannot operate simultaneously against cruise and ballistic missiles; defensive responsibilities must be split between the two ships. We examine three alternatives: operations with divided duties, independent operations using a shared common operating picture (COP), and coordinated operations using a cooperative engagement capability. Figure S.2 illustrates each.

**Platform-Centric Operations, Divided Duties:** The two cruisers operate almost autonomously. That is, although they remain in contact with each other, no mechanism on board either ship automatically shares information on the arriving threat and/or firing solutions and no central authority directs the defensive response. Both ships employ a first-in-first-out (FIFO) queue discipline policy for engaging incoming missiles. For cruise missiles, this makes self-preservation

RANDMR1449-S.2



NOTE: The Aegis cruisers operate in pairs with one directing its SPY-1 radar to detect and track ballistic missiles, while the other directs its SPY-1 radar to detect and track ASCMs.

Figure S.2—Alternative Operating Procedures

collective. This means the ship designated to intercept cruise missiles does not give itself priority against attack.

**Network-Centric Operations, Shared COP:** In the shared COP mode, both ships can see incoming ballistic missiles and cruise missiles. An understanding exists between the two ships concerning the nature of the attack. Connectivity has been extended so that missile threat trajectory and arrival time information are shared electronically, and in this sense the two ships can collaborate. Although sensor information is shared, the two ships continue to operate independently. Both ships have cruise missile and ballistic missile defense responsibilities. As a result, poor “queue discipline” is likely because both ships may engage the same missile or fail to engage a missile that might have been engaged with better coordination.

**Network-Centric Operations, Cooperative Engagement:** This is the most compelling option and therefore is analyzed most fully. Both ships have access to complete defense solutions, and allocation of ships to targets is controlled centrally by one of the two ships engaged in the operation. We depict a separate node for this additional function for the controlling commander. Not only connectivity is required in this case, but also automated systems to assess the relevant factors that go into making the best decision. Both ships have cruise missile and ballistic missile defense responsibilities, as in the previous case.

## Decisions

The decisions center on the allocation policy that best protects both cruisers and the critical infrastructure targets. Remaining inventories of SM-2 Standard missiles on board each ship are critical to the decision process. The consumption rate for these missiles depends on the length of the time period, the firing rate, the shooting policy, and the number of ships engaging each enemy missile. Dedicated anti-cruise missile (ACM) or anti-ballistic missile (ABM) ships may risk emptying their defensive magazines before the attack has concluded. To prevent this, the two ships could then reverse roles.

**Platform-Centric, Divided Duties:** Only the role-switching decision is modeled for this case. The decision to switch or not is made at the beginning of each period. The need to switch roles is based on re-

maintaining inventories of Standard missiles on either of the defending cruisers.

**Network-Centric, Shared COP:** Both ships act independently—but with shared information. Each ship engages the targets it feels it can best intercept. The decision to engage an enemy missile is based primarily on the relative location of the ship and the enemy missile. Consideration is also given to remaining inventories of missiles and the anticipated attack arrival rate for the next period.

**Network-Centric, Cooperative Engagement:** The decision to be made is which ship(s) should attempt to intercept each incoming cruise missile and how many missiles can each “safely” engage in each period. The difference between this decision and the shared COP case is that, in this instance, a central control authority makes the decision based on shared information from both ships. The assignment of ship(s) to conduct the defense against cruise missile attack is determined using a set of decision rules based on allocating ships to missiles to prolong the survivability of the cruisers while maintaining inventories of ACMs and ABMs as long as possible.

## Mathematical Representations

Network complexity and collaboration are combined to provide an estimate of the number of cruise and ballistic missiles expected to arrive in the next and subsequent periods. These estimates are then used in the allocation decision rules. The estimates are as follows:

$$\hat{\lambda}_c = (1 - K_{cC_v}(\lambda)) \frac{n_c}{T} + K_{cC_v}(\lambda) \lambda_c$$

$$\hat{\lambda}_b = (1 - K_{cC_v}(\lambda)) \frac{n_b}{T} + K_{cC_v}(\lambda) \lambda_b$$

The terms  $\hat{\lambda}_c$  and  $\hat{\lambda}_b$  are the current estimates of the arrival rates of attacking cruise and ballistic missiles respectively.  $K_{cC_v}(\lambda)$  represents the knowledge about the attack distribution informed by the complexity of the network and the collaboration that has taken place. The subscript  $v$  refers to the case being examined ( $v = 1$ —platform-centric,  $v = 2$ —COP, and  $v = 3$ —cooperative engagement).  $\lambda_c$  and  $\lambda_b$  are the true attack distributions and  $n_c$  and  $n_b$  are the attack

sizes for cruise and ballistic missiles to be launched over a total of  $T$  minutes. The knowledge function is bounded between 0 and 1 with  $K_{CC_v}(\lambda) = 1$  representing perfect knowledge. When this occurs,  $\hat{\lambda}_{ci} = \lambda_{ci}$  and  $\hat{\lambda}_{bi} = \lambda_{bi}$  and when knowledge is poor ( $K_{CC_v}(\lambda) = 0$ ) we have that  $\hat{\lambda}_{ci} = n_c/T$  and  $\hat{\lambda}_{bi} = n_b/T$ . This last case means our estimate is that the missiles are uniformly distributed over the attack horizon,  $T$ . These equations are the MOP. The effectiveness measures (survivability of cruisers and infrastructure) are assessed as a result of the decisions taken based on these measures.

### A TIME-CRITICAL TARGET

The second vignette focuses on the problem of locating and destroying an enemy submarine Type 877 Kilo in a short period of time. It is known in advance that the Kilo will leave port to replace another enemy submarine killed by a U.S. SSN, and a plan is devised to kill it before it can threaten the SLOCs. Figure S.3 depicts the situation on D+10, the day the enemy submarine leaves port en route to a position north of the friendly island to menace shipping along the SLOCs. On D+6, a *Virginia*-class SSN begins a previously planned Intelli-

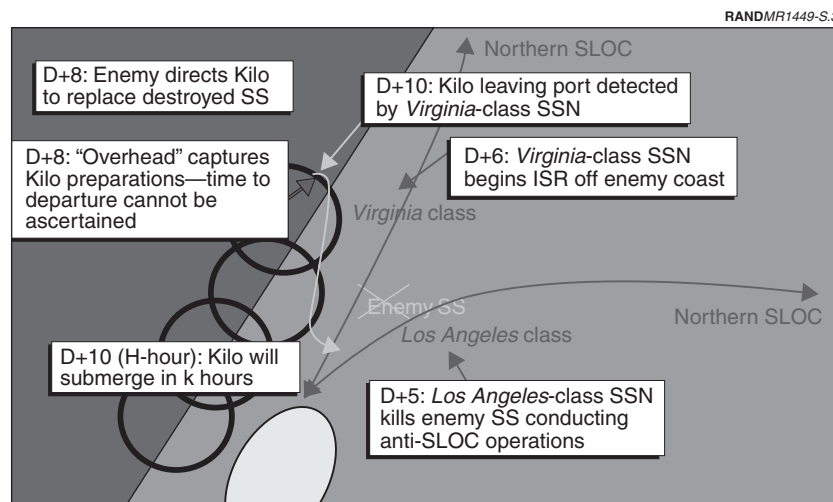


Figure S.3—Situation at D+10

gence, Surveillance, and Reconnaissance (ISR) mission off the enemy's coast. On D+10, it detects the Kilo leaving port and is able to track it as it moves toward its final station. The objective is to kill the Kilo on the surface as it emerges from the port without revealing the ISR submarine or disrupting its mission. An F/A-18 fighter attack aircraft will be vectored to the Kilo and will kill it using a Standoff Land-Attack Missile—Extended Response (SLAM-ER) missile.

### Measures of Performance and Force Effectiveness

The Joint Task Force Commander (JTFC) has determined that catching the Kilo on the surface and attacking it as early as possible can best accomplish his objective. The command and control MOP therefore is *Time on Target*—the time available to an attacking aircraft to conduct its attack measured as the time elapsed between its arriving on station and the Kilo submerging. The combat MOE is the *probability that the SLAM-ER destroys the Kilo*.

**Platform-Centric Operations.** In this configuration, the ISR SSN reports to the operational commander, who would then alert the two CVBGs in the area that a threat submarine has left port. An F/A-18 is placed in “Alert 5” status and flies out to attack the Kilo from one of the CVBGs. The ISR SSN continues to provide updates on the Kilo through his operational commander. Command and control is split between the SSN and air operations personnel on the carrier. The SSN may attack the submerging Kilo without notifying other units. On the other hand, air operations might determine that the threat level to the aircraft was becoming excessive and abort the mission.

**Network-Centric Operations.** In this case, the connectivity among the participants is richer. The ISR submarine has two-way communications (via Link 16) to the carriers and the deploying aircraft. The controlling carrier uses two-way communications with the F/A-18 to control its operation and to confirm threat status updates. The F/A-18 receives periodic target updates directly from the ISR submarine. The command and control architecture has the same divisions as the platform-centric operation architecture, but consequences of this division are considerably reduced. For example, the ISR submarine may still decide that the Kilo is about to submerge and that the aircraft cannot attack in time and attack the Kilo itself. However, with communications directly to the carrier, and to the aircraft, the air-

craft can be turned back earlier. Similarly, if air operations determines that the threat to the F/A-18 is excessive and it is turned back, the ISR submarine can be alerted in its next communication cycle and therefore have more time to attack the Kilo itself.

**Future Network-Centric Operations.** The Navy's Unmanned Combat Aerial Vehicle (UCAV) concept is currently under consideration by the Office of Naval Research (ONR). UCAVs are designed to be launched from a variety of surface combatants and therefore eliminate the burden of keeping an F/A-18 (and a catapult) on alert status for days. After the ISR submarine detects the Kilo coming out of port it alerts all potential UCAV launch ships. The ships receiving the message negotiate to determine which can get a UCAV to the Kilo first. Such issues as who makes the final selection, who determines when sufficient collaboration has occurred, what prior designations have been made, what is the polling frequency, and who determines which combatants with UCAVs are candidates are command and control procedural questions that must be addressed and evaluated analytically. A UCAV is then launched and begins to fly out to the Kilo Area of Uncertainty (AOU). The ISR submarine takes over control of the UCAV, including weapon release. The command and control architecture for this case is unsettled. Several options are available and constitute the basis for conducting exploratory analysis to determine the effects of each on combat outcomes.

### Mathematical Representations

As with the missile defense vignette, network complexity and collaboration combine to affect combat operations. In this case however, the decision to attack is based on an assessment about the time required to get an attack platform (UCAV or F/A-18) in position to launch a weapon. The expected latency expression is as follows:

$$L_{cC} = \frac{1}{1-g(C)} \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} [(1-K_j(t))^{\omega_j}] \frac{\delta_i}{\lambda_i},$$

where  $L_{cC}$  is the expected time required to get the attack platform on station given the effects of collaboration and network complexity. Table S.1 describes the terms in this expression. This is the MOP.

**Table S.1**  
**Definition of Terms for TCT MOP**

Term	Definition
$g(C)$	The complexity factor ( $0 \leq g(C) < 1$ ). Measures the effects of “information overload.”
$\tau$	The number of entities (nodes) participating in the operation.
$d_i$	The indegree of node $i$ , i.e., the number of connections that terminate at node $i$ .
$K_j(t)$	The knowledge gained from node $j$ ( $0 \leq K_j(t) \leq 1$ ).
$\omega_j$	The importance of node $j$ . $\omega_j = 1$ if node $j$ is participating in the operations and $\omega_j = 0.5$ if it is not.
$\delta_j$	If node $i$ is connected to node $j$ , $\delta_j = 1$ otherwise $\delta_j = 0$ .
$1/\lambda_i$	The mean time to complete the task required at node $i$ .

The effectiveness of the operation depends on the probability that the enemy submarine will be detected and successfully engaged. This in turn depends upon the amount of time,  $T = S - L_{cC}$ , available to search and attack, where  $S$  is the time the submarine will submerge. We assume that the SLAM-ER is sufficiently effective so that if it detects a target, the target is destroyed with certainty. The MOE therefore is based on the search equation:

$$P_d(T) = 1 - e^{-\gamma T},$$

where  $P_d(T)$  is the probability the submarine will be detected in  $T$  minutes or less. The coefficient  $\gamma$  consists of the geometrical aspects of the problem, such as the AOU, the sensor’s field of regard, and its sweep width. Also, it includes the information update frequency from the ISR SSN and knowledge gained from external sources.

### EXPLORATORY DATA ANALYSIS (EDA)

Changes in MOEs that result from modifying the levels of input variables are best understood by using visualization techniques. By varying the input variables, we can better understand the structure of the data and the complex relationships between inputs and MOPs/MOEs. This is most easily achieved by using a single representative value for some subset of inputs—essentially treating them

as fixed and assigning two of the input variables to the x- and y-axes. Exploration is then conducted by interactively changing the fixed input values to better understand the relationship between that variable, the input variables shown on the axes, and the resulting MOE. A complete EDA has three phases:

- **Phase I—an introductory visual exploration:** This allows all possible inputs to occur with equal probability.
- **Phase II—a focused analysis:** The goal is to restrict the exploration to ranges of input variables that are more likely to occur.
- **Phase III—a full-scale stochastic simulation:** The simulation does not use the expected value of known distributions, but rather randomly draws from them at each simulation replication.

The EDA tool developed for this study focuses on the first two phases, where important relationships are discovered and the expected impact of policy decisions can be made before undertaking the more costly task of simulation.

## CONCLUSION

We conclude as we began by stressing the need for new measures and metrics that incorporate the effectiveness of C4ISR systems, procedures, and equipment and their effect on combat outcome. The assertion is generally made that a richly connected network of C4ISR facilities and weapon systems will improve decisionmaking and therefore favorably impact combat operations. This may be true, but as yet we have no systematic, universally accepted way to demonstrate the truth of this claim. This report has focused on the Navy's early attempts at codifying one approach. Clearly, much remains to be done before accepted practices can be established. The work presented here is just a beginning.

## Networks and NCW

NCW is not just about networks. Networks are necessary but not sufficient to ensure effective network-centric operations. Much has been made of the relationship between the “size” of the network and its efficiency. The computer network analogy is often cited to illus-

trate that a more richly connected network *ipso facto* improves overall performance.

A somewhat opposite claim is that the larger the number of connections in an operational network, the more likely individual nodes will experience “information overload.” Both arguments are compelling. However, it remains to be seen if either is true when applied to military operations.

In this work, we suggest a way to assess both the good and bad effects of complexity with no claim that our representations are accurate. However, complexity alone, as defined by the number of connections in a network, is clearly not enough to assess the effectiveness of network-centric operations. The *command and control procedures* implemented on the network and the quality and extent of *collaboration* also play an important role.

Collaboration is expected to improve a process by which a team of individuals work together to achieve a common goal. We have argued that collaboration is important because it can enhance the degree of shared awareness in a group focused on solving a specific problem or agreeing on a decision. Although we have assumed that collaboration is generally beneficial, we have also recognized that it is not *uniformly* beneficial.

### **Information Theory**

Information theory is not just a subset of communications theory, as some suggest. Rather it contributes to several fields of human endeavor, but, most important, it applies to military operations. In this work, we rely on information theory to assess the “amount” of knowledge available in a command and control system. To do this, we apply the important concept of information entropy or Shannon entropy.

The quality of collaboration is clearly related to the knowledge the participants in the decision team about the uncertain environment in which they operate. It is natural therefore to resort to the knowledge function, which is derivative of information entropy, to assess the effectiveness of the collaboration between two decision team members.

## **Next Steps**

We have stated repeatedly that this is but a small first step in the effort to establish measures and metrics to connect C4ISR and network-centric operations to outcomes of combat. As a next logical step, the following areas should be researched:

- Improve understanding of network complexity and better characterize its effects.
- Improve understanding of the effects of collaboration.
- Examine ways to represent the multidimensional effects of collaboration.
- Assess the effects of information quality on the effects of collaboration.