A MATHEMATICAL FRAMEWORK FOR MEASURING THE EFFECTS OF INFORMATION AND COLLABORATION ON SHARED AWARENESS[1]

Walter Perry, Ph.D.
Senior Analyst
RAND
1200 South Hayes Street
Arlington Virginia 22202
Tel: (703) 413-1100 X 5228
Fax: (703) 413-8111
e-mail: Walter_Perry@rand.org

David Signori, Ph.D.
Senior Analyst
RAND
1200 South Hayes Street
Arlington Virginia 22202
Tel: (703) 413-1100 X 5400
Fax: (703) 413-8111
e-mail: David_Signori@rand.org

Abstract

The military is formulating new visions, strategies, and concepts that capitalize on emerging information age technologies. New networked C4ISR capabilities promise information superiority and decision dominance but assessing their contributions toward achieving a network centric warfare capability is still a major challenge. DoD is exploring ways to create and leverage information superiority by characterizing conditions under which it can be achieved thus gaining a competitive advantage. This requires a definition of concepts, metrics, hypotheses and analytical methodologies that can be used to focus research efforts, compare alternatives, and measure progress. This paper outlines some first steps toward doing this by quantifying information superiority concepts that up to this point have been abstract or vague. Conceptual models for transfer functions that could be tailored to specific applications were developed and linked. The models incorporate metrics that measure the quality of products produced by the several C4ISR processes. The methodology is partitioned into three segments. The first quantifies key features of the real world. The second quantifies the quality of information as it transits the sensors, fusion centers, and distribution networks of the C4ISR infrastructure. The third quantifies the impact of the resulting quality of information on the degree of shared awareness.

INTRODUCTION

The military is formulating new visions, strategies, and concepts that capitalize on emerging information age technologies to provide its warfighters with significantly improved capabilities to meet the national security challenges of the 21st century. New networked Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities promise information superiority and decision dominance that will enhance speed of command and enable revolutionary warfighting concepts. Assessing the contribution of C4ISR toward achieving a network centric warfare capability is a major challenge for the

---

[1] This paper summarizes the work reported in a forthcoming RAND publication: [38] Perry, Signori and Boon.

Department of Defense due to the multiplicity of interacting factors and the lack of understanding of the fundamentals associated with information superiority concepts. DoD is embarked on a journey of exploration to discover how to create and leverage information superiority by characterizing conditions under which it can be achieved and a competitive advantage can be gained. Much like the development of a new branch of science, this requires a definition of concepts, metrics, hypotheses and analytical methodologies that can be used to focus research efforts, compare alternatives, and measure progress.

In this paper, we take a small step toward solidifying and *quantifying* some information superiority concepts that up to this point have been abstract or vague. Specifically, the focus is on both the quality of information, its processing, and some of the cognitive aspects of achieving individual and shared situational awareness. The quantitative methodology and illustrative mathematical representations in the paper are mostly theoretical and therefore they should be treated as hypotheses requiring subsequent experimental testing. Also the illustrations relate to force-on-force combat operations as opposed to a broader range of operations that includes Operations Other than War (OOTW) or asymmetric warfare. However, aspects of the approach apply more widely and provide a basis for informed dialog that, in our view, will eventually lead to more comprehensive and validated capabilities to quantitatively explore the impact of improved C4ISR systems and processes on operational outcomes.

The research reported here builds on the work of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C3I) Information Superiority Metrics Working Group (ISMWG). This body has been attempting to define working definitions, specific characteristics and attributes of key concepts and the relationship among them that are needed to measure the degree to which information superiority concepts are realized and their impact on the conduct and effectiveness of military operations. Such an endeavor requires a common language and a set of integrated hypotheses as well as metrics, instruments and tools to collect and analyze data such as those suggested in this work.

THE DOMAINS

C4ISR is conceptualized as consisting of three domains: *physical* (ground truth), *information* and *cognitive*. The C4ISR process is seen as extracting data from ground truth, processing the data in the information domain to produce a common operating picture (COP), deciding on a course of action and executing the decision. The quality of the COP produced in the information domain coupled with the quality of collaboration in the cognitive domain is used to heighten shared situational awareness. Data about ground truth obtained from the collection process in the information domain is *transformed* into a COP that contributes to enhanced situational awareness in the cognitive domain. The transformations are processes that include data collection and processing, data fusion and dissemination of information. These processes are not discussed here. We assume they are performed and we focus instead on the *quality* of the information and products they produce.[2] Individual situational awareness, the quality of the information in the COP, the prior experience of the decision making team and the degree to which they collaborate successfully all contribute to shared situational awareness.

---

[2] For a complete discussion of C4ISR information processing algorithms, see [39] Perry and Sullivan.

The focus is on the collection of data, the processing of collected data to produce the COP, the dissemination of the COP from the various fusion facilities to the ultimate users, the prior experience of the decision making team, the quality of their collaboration and finally, the impact of all of this on shared situational awareness. Clearly, this is not the end of the story. Several important aspects of the decision making cycle such as *decision* and *synchronization* are not treated. In addition, the relation between awareness and understanding, and how understanding affects decision and action are deferred to future work. Nevertheless, this paper presents a new and important methodology for assessing the quality of information and ISR processes in general as well as some of the more psychological aspects of the decision making process. It is based on sound mathematical concepts and hypotheses from the literature and therefore provides a foundation for further inquiry. In the process, illustrative mathematical relationships are suggested that will require verification and refinement through experimental and operational data.

The measures and metrics proposed are presented within the context of the three domains. Figure 1 depicts the concepts defined in what is referred to as the Information Superiority Reference Model. The sensors, fusion process and dissemination networks transform ground truth from the physical domain into an observed COP that is essentially an approximation to ground truth. This time varying estimate is used by one or more humans working alone or together to develop an awareness of the current and future situation that can be used to gain understanding of opportunities and subsequent decision making regarding an appropriate course of action. The ground truth, the observed COP and the mental image held by decision makers are characterized by a set of features described by information whose quality must be measured as it is transformed throughout the process. The process is cyclic in that the decision emanating from the cognitive domain eventually affects ground truth thus possibly altering the features of interest to the subsequent decision processes.

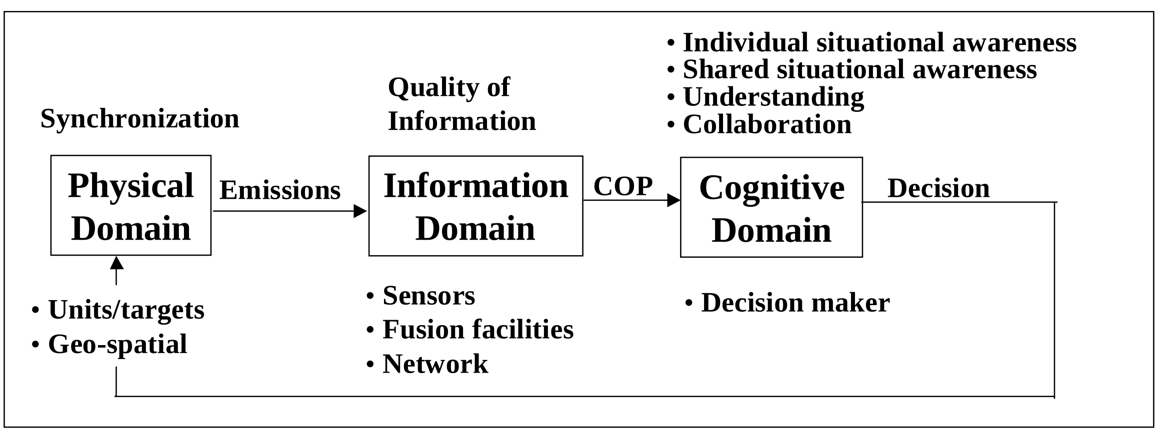

Fig. 1 –C4ISR Reference Model

A distinction is made between the *quality* of information and its *value*. The quality of information involves those measures that are *independent* of the specific decisions being made. This is in contrast to the value of information, which depends strongly on a specific decision making context. The latter will determine which elements of information and which metrics for assessing the quality of the information are important as well as the range of values that are most critical to the decision maker. The former however, provides a more general point of reference that can be useful in exploring a wide spectrum of situations to determine, for example, where in the quality space value is provided for in various situations.

Another distinction can be made between information quality and the quality of the process that generates information. Both are important to this discussion and in the definitions and examples discussed below, both are described without further explanation.

There are several measures of information quality. For this work however, we focus on three: *completeness, correctness* and *currency*. Their definitions are as follows:[3]

Def 1: *Completeness* is the degree to which the information received and transmitted is free of gaps.

Def 2: *Correctness* is the ability of the ISR system and fusion process to discern "truth". That is, the degree to which the information agrees with ground truth.

Def 3: *Currency* is the time required for the ISR system and the fusion process to produce a common operating picture of the combat situation.[4]

THE INFORMATION DOMAIN

The Information Domain contains all of the information collection, processing and dissemination facilities. It is further subdivided into three sub-domains: *sensor (ISR), fusion* and *network* and these three comprise the main effort of the C4ISR system. Figure 2 depicts the process as a set of mathematical transformations that serve to illustrate the remainder of the discussion in this domain.

Features

A feature is defined to be a prominent part or characteristic of the combat situation. Features are extracted from the physical domain and serve as the building blocks that make up the COP. Consequently the collection of features must be sufficient to communicate to the commander the current estimate of the combat situation. ([28] Mitchie)

Although the sensors and sources can be cued to collect information to support specific decisions, in general, we view the collection of feature vectors sufficient to support all decision on the battlefield. When focusing on a specific decision, the information elements of interest, a subset of the feature vectors, are those that are *valuable* to the decision. The quality of the information in the COP in this case is the quality of this subset. Most notably, currency is replaced by timeliness as the measure of information latency.

The common picture of the *i*th enemy unit/target at time *t* is defined in terms of a general set of features represented mathematically by the row feature vector $\mathbf{F}_i(t) = [f_{1i}(t), \cdots, f_{ni}(t)]$. The elements of this vector are features such as the location, type, speed, direction, etc. of a target. Similarly, the common picture of the geo-spatial aspects of the physical domain at time *t* is

[3] These and subsequent definitions are constantly undergoing refinement and therefore are subject to change. We present them here in this form both to structure the discussion and to solicit comments from readers.

[4] We use the term "currency" as opposed to "timeliness". Timeliness is situation dependent in the sense that the decision maker specifies when certain information is required. Currency, as defined here, is independent of the situation and is therefore consistent with our definition of information quality.

defined as the row feature vector $\mathbf{G}(t) = [g_1(t), \cdots, g_k(t)]$. The perceived situation can be represented using estimates of each of the features for each enemy unit/target perceived to be in the area of operations (AO) and the current estimate of the geo-spatial features. The COP then is expressed as the matrix $\mathbf{F}(t) = [\mathbf{F}_1(t), \cdots, \mathbf{F}_m(t), \mathbf{G}(t)]$. The quality of the information in the vectors will depend upon the completeness, correctness, currency, etc. of the data provided by the sensor suite and how well the data is processed and analyzed.

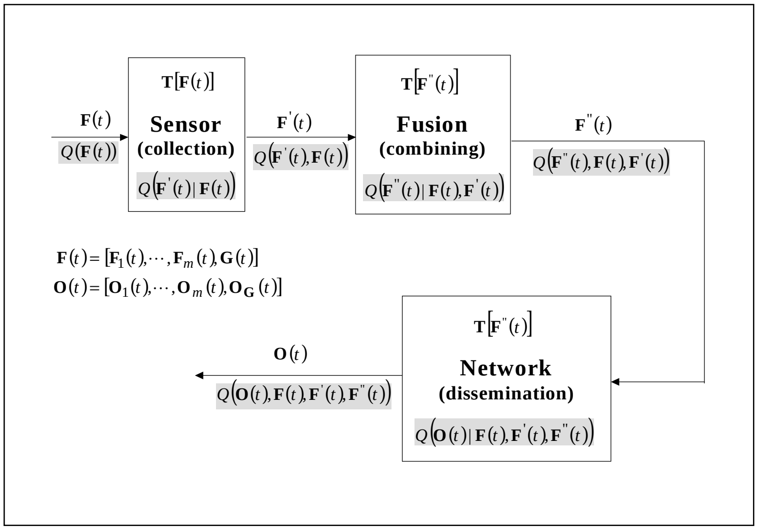

Fig. 2 –Information Domain Transformations

Quality Transformations

Note that in each sub-domain, there are two transformations occurring simultaneously: *process* transformations and *process quality* transformations. The former consists of the procedures, algorithms, communications protocols, network architectures, etc. that transform data into information and subsequently inform awareness. These are denoted $T(\bullet)$. Process transformations are included for completeness in Figure 2, but other than acknowledging that they exist, we do not treat them in this work. Quality transformations, denoted $Q(\bullet)$, are the subject of this research.

Completeness and Correctness: Quality transformations illustrate how the correctness and completeness of the process outputs are transformed. In this case a simple conditional probability model is used. $Q(\bullet)$ represents the quality of information produced at one of the information sub-domains. The correctness and completeness of the information on output at each of the sub-domains is given by the following chained conditionals:

Sensor sub-domain: $Q(\mathbf{F}'(t), \mathbf{F}(t)) = Q(\mathbf{F}'(t) \mid \mathbf{F}(t)) Q(\mathbf{F}(t))$,

Fusion sub-domain: $Q(\mathbf{F}''(t), \mathbf{F}(t), \mathbf{F}'(t)) = Q(\mathbf{F}''(t) \mid \mathbf{F}(t), \mathbf{F}'(t)) Q(\mathbf{F}(t), \mathbf{F}'(t))$,

Network sub-domain: $Q(\mathbf{O}(t), \mathbf{F}(t), \mathbf{F}'(t) \mathbf{F}''(t)) = Q(\mathbf{O}(t) \mid \mathbf{F}(t), \mathbf{F}'(t) \mathbf{F}''(t)) Q(\mathbf{F}(t), \mathbf{F}'(t) \mathbf{F}''(t))$.

The "quality of ground truth", $Q(\mathbf{F}(t))$, is taken to be 1.0. Because the conditional quantities developed as metrics are defined on the interval [0,1] we make the analogy to probability theory and treat the transformations as conditional probabilities.

Currency: Unlike completeness and correctness, currency is not treated as a probability and therefore a conditional probability model does not apply.[5] Units of time is the metric. Although the currency in one sub-domain may depend on the currency of the previous sub-domain, it need not. The time required to complete a process may be totally dependent upon the complexity of the process, the sub-domain architecture and the resources applied to the tasks required. Within each domain, tasks may be completed in series or in parallel therefore affecting the overall time required to complete sub-domain processing. In some cases, tasks in different sub-domains may proceed in parallel as well, e.g., sensing and fusing. The appropriate model for analyzing currency within each sub-domain and for the overall system therefore is the critical path method (CPM) ([49] Wagner).

THE SENSOR SUB-DOMAIN

Information about the physical domain originates with the sensors and information sources allocated or directed to the area of operations. Sensors are designed to detect objects, record images of designated areas and estimate physical phenomena. They are capable of performing surveillance and reconnaissance over large areas in a systematic fashion, subject to the existence of threats that may jeopardize the survival of their platforms. Sensors may be capable of detecting types or classes of militarily relevant objects or targets, or may detect whole classes of objects, such as moving vehicles. In general, sensor performance is a function of the environment (terrain, foliage, electromagnetic background noise, extraneous reflected sunlight or glint, etc). For example, radar sensors that operate in the microwave band can only detect targets that have a radar cross section above some minimum threshold and in environments where the signal-to-noise ratio is also above some minimum threshold.

Sources, on the other hand, may be covert and typically operate over much smaller areas. Sources include such things as human observations, very short range communications intercepts or surveillance, unattended covert devices that can be read out intermittently, a priori knowledge about enemy force dispositions, future plans, etc.

Sensor Models

A wide variety of sensors are typically available and used in military operations. Each has its strengths and weaknesses. The generic model of sensor performance used in this analysis is composed of probabilities of detection as a function of range. Target location and velocity errors (direction and speed) are also expressed as a function of range. Figure 3 depicts a model of sensor detection performance. A typical sensor with an unobstructed view of the battlespace will have a minimum and maximum range. Within this range band it is capable of detecting targets of a type specific to its technical capabilities, that is, it will have a non-zero probability of detecting its designated targets. In the diagram, we have the following functional relationship:

---

[5] This is clearly not universally true in that the time to perform a task can very easily be random and as mentioned, may depend upon the randomness of previous tasks.

$$P(d)=\begin{cases} k \text{ if } d_{\min} \le d < d_b \\ f(d) \text{ if } d_b \le d \le d_{\max} \\ 0 \text{ otherwise} \end{cases}$$

The sensor achieves its maximum capability, $P(d)=k \le 1$, at the minimum range and maintains that capability through the range, d_b. Performance begins to fall off beyond d_b according to some relationship that may be a function of several factors, including target aspect angle relative to the sensor, target state (temperature, velocity, configuration, etc.) and the state of the immediate and intervening environment. The performance of many sensor types can be modeled with this generic profile.[6]

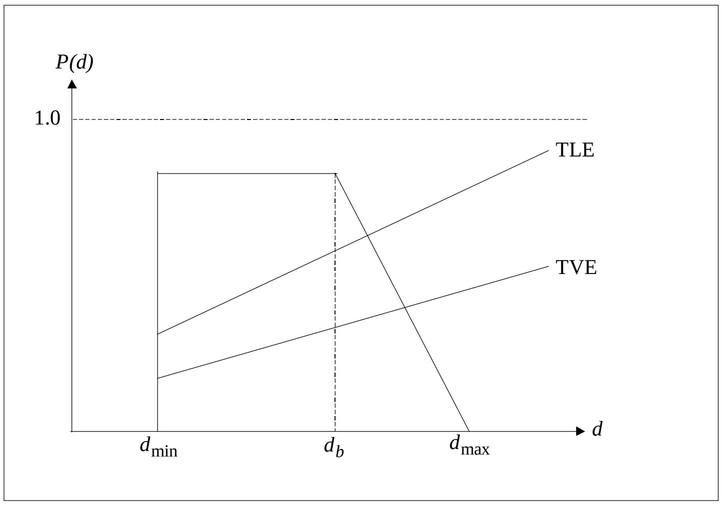

Fig. 3 –Generic Sensor Performance Model

The problem then is to examine the nature of the functional, $P(d)$ for each sensor and for the entire suite. One way to do this is to assess the reliability of the sensor and the sensor suite. We let $P(d)=R(d)$ be the *reliability* of the sensor where *d* is the distance from the sensor to the target. Generally, the independent variable is time, but it need not be. In the case of sensors, distance is much more useful in that it can account for mal-positioned sensors, inefficient multi-sensor configurations and it generally characterizes sensor detection performance. The general form of $R(d)$ is:

$$R(d)=e^{-\int_0^d r(s)ds},$$

where $r(s)$ is called the failure rate function and is dependent upon the characteristics of the sensor and the current operating situation. Sensor characteristics include the ability to detect, estimate and classify targets. Note that for $d=0$, $R(d)=1$. That is, when the sensor is co-terminal with the target, it is infallible. This is of course, an idealization, and therefore to

[6] The two lines (TLE and TVE) refer to target location error and target velocity error. Both increase with increasing range. Their use in this analysis is discussed more fully in the correctness measure discussed below.

conform more closely to the generic model depicted in Figure 3, we recast the reliability function as the decreasing segment in a piecewise relationship so that we now have:

$$R(d) = \begin{cases} 0 \text{ if } d \le d_{\min} \\ e^{-\int_{d_{\min}}^{d} r(s)ds} \text{ otherwise} \end{cases}.$$

Note also that $R(d)$ is a probability that can be interpreted as the probability of detection at a range d.[7] In this formulation, $d_{\max}$ is reached only in the limit. This is not much of a problem however since the rate of decline of $R(d)$ for $d > d_{\min}$ is controlled by $r(s)$.

Expressing sensor detection probability in this way is extremely useful. For example, the effects of occlusions can be modeled through the appropriate selection of $r(s)$ so that for a totally occluded view, $d \to \infty$ and for impaired views, such as foliage, atmospheric disturbances, etc., d is set to be larger than the physical distance between the sensor and the target. This suggests that $r(s)$ might be defined piecewise to reflect the effects of occluded views. We pursue this more fully next.

Occlusions

A sensor is occluded when terrain and/or foliage intervene between the sensor and the target. Most sensors require a clear unobstructed view of the target. We can use the reliability function to model the probability of detection for different levels of occlusion without resorting to complex surface maps. For example, suppose the failure rate for a given sensor without occlusions is $r(s) = 1$. This produces a detection probability function $R(d) = e^{-d-d_{\min}}$. We can now express the effects of occlusions by damping $R(d)$ so that $R(d) = ke^{-d-d_{\min}}$, where $k \in [0,1]$. For $k = 0$, we have a totally occluded sensor and, as mentioned above, $R(d) = 0$ at all distances. For $k = 1$, no occlusions exist and we get the basic relationship. All other values of k reflect varying levels of occlusion and their effect is to reduce the probability of detection.

Another use of $r(s)$ is to assess the effectiveness of *sensor tasking*. When sensors are tasked to focus on a particular aspect of the battlespace, the practical effect is to reduce the distance between the sensor and the target – thus improving the reliability of the tasked sensors. For example, if $r(s) = 1$ as in the example above, the probability of detection at 1 km from the target is $R(1) = 0.368$. Suppose this is the closest the sensor is able to approach the target and further suppose that only sensors with similar failure rates are available. If we task three of these to observe the target, the detection probability becomes: $R(d) = 1 - (1 - .368)^3 = 0.748$. For a sensor of this type, this is equivalent to being approximately 0.3 km from the target therefore $R(0.3) \approx 0.748$.

---

[7] There are several good texts on reliability engineering. See [4] Ayyub and McCuen, and [32] Pecht, for example.

Sensor Quality Transformations

Figure 2 depicts the transformation of ground truth data into pre-fused information in the first process block. The transformation is a result of the sensor suite operating on the AO. The information quality transformation is depicted as the conditional probability, $Q\left(\mathbf{F}'(t) \mid \mathbf{F}(t)\right)$. The objective is to mathematically construct this quantity using the model described above.

Measure of Completeness: *the degree to which real targets in the AO are detected*

This measure as applied here focuses on "real" targets only – not detections of false targets or decoy, or of non-combatant vehicles. Although we realize that some sensors, will detect many objects that are not militarily relevant, the degree to which an individual sensor or suite of sensors can distinguish military targets from other similar objects is the subject of the correctness performance measure discussed below. What is relevant to the completeness measure is the degree to which military targets are *not* detected.

Metric for Completeness: *the fraction of real targets detected in the AO*

The implication is that either the true number of unit/targets in the AO is known, or an estimate is available. Given that the true number is almost always not known – except for controlled experiments, we assume the latter and therefore focus on developing estimates. For an individual sensor, S_i, the percentage of real targets detected is $R_i(d)$ as developed above. Hence, if the sensor suite consists of a single sensor, and if correctness is ignored, we get $Q\left(\mathbf{F}'(t) \mid \mathbf{F}(t)\right) = R_i(d)$. However, the architecture of must the entire sensor suite greatly affects the metric and therefore we discuss this next.

The better the sensor suite (in terms of sensor performance and operational integration), the more likely the number of targets detected will be the total in the AO. We have an expression for the fraction (reliability) of targets detected for an individual sensor, $R_i(d)$; what is needed now is an assessment of the integrated sensor suite. Figure 4 depicts three operational modes or sensor architectures: *independent* operation, *cueing* and *mixed mode*.[8] The structure of the network is exemplary. The fact that all reports end at a single fusion center is not central to the assessment. Clearly, fusion can take place anywhere in the ISR and fusion system and it may be distributed or centralized.

---

[8] This may not be an exhaustive set. For example, a standby configuration is also possible in which a sensor of less reliability is held in reserve to temporarily replace a more reliable system that has failed. See for example, [15] Dhillon.

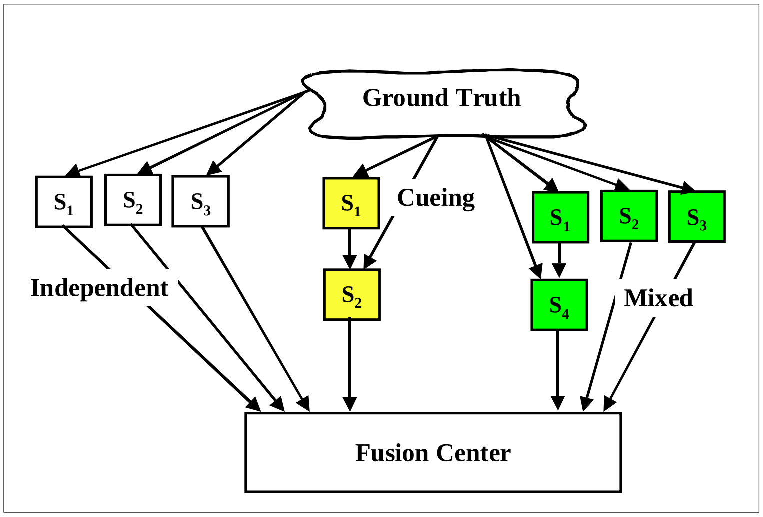

Fig. 4 –Multi-Sensor Operations

Independent Operation: This is the simplest form of operation. Each sensor observes the area of operations independently and reports its detections to the common fusion center. This is essentially parallel operation in reliability analysis and it increases the likelihood that a detection will occur. To calculate the sensor suite reliability for this case, we get:

$$R(d)=1-[1-R_1(d)][1-R_2(d)][1-R_3(d)].$$

Cueing: In cueing operations, one sensor detects a target and notifies another to confirm the detection (or in practice, to provide additional data on the target). A report is rendered when the two sensors have detected the target. Because two sensors must "see" the target before a report is rendered, the reliability of this mode of operation (in terms of generating a detection) is reduced. This is equivalent to a system operating in series and therefore the system reliability is:

$$R(d)=R_1(d)R_2(d).$$

Mixed Mode: This is the most likely operational mode, a mixture of both independent operations and cueing. The overall system reliability in this case is dependent upon the complexity of the system structure. For the simple case depicted in the diagram, we get:

$$R(d)=1-[1-R_1(d)R_4(d)][1-R_2(d)][1-R_3(d)].$$

From this we have that the completeness metric for sensors is $Q_{com}\left(\mathbf{F}'(t)\,|\,\mathbf{F}(t)\right)=R(d)$.

Measure of Correctness: *the degree to which the true target features approximate their ground truth values*

Correctness is measured as a deviation from ground truth. This is sometimes referred to as "accuracy" and indeed; there is little difference in the two terms. We prefer to use correctness in that it appears to be less absolute. Clearly, deviation from ground truth implies that either ground truth is known and therefore measurement is trivial, or it is not known and other techniques for evaluating an estimate must be employed. We define metrics for both cases.

Metric for Correctness: *the amount of bias in an estimate of a feature*

The estimates for each of the features in the feature vectors are, in most cases, the means of probability distributions describing the uncertainty about the features.[9] For non-quantitative features, we use the mode as the estimator. This suggests that we rely on *estimation theory* as the basis for evaluating the quality of these estimates. There are several techniques. The most obvious is the degree of bias in the estimate.[10] If $\theta(t)$ is the parameter we are estimating at time *t*, then $A(t)=\hat{\theta}(t)-\theta(t)$ is the bias in the estimate where $\hat{\theta}(t)$ is the estimator. This is a useful tool to evaluate the correctness of alternative sensor architectures during controlled experiments. Under these conditions, ground truth is known and therefore the bias can be calculated. The mean is an unbiased estimator in that $E\left|\hat{\theta}(t)\right|=\theta(t)$. This makes the sample mean an unusually good estimator to use since we are guaranteed that for large sample sizes, the bias tends to 0. A suitable metric in this case therefore is the normalized bias or $Q_{cor}\left(\mathbf{F}^{'}(t) \mid \mathbf{F}(t)\right)=\frac{|A(t)|}{\theta(t)}=\alpha(t)$.

Metric for Correctness: *the degree to which estimates are tightly clustered*

However, other metrics can be developed using the variances of the estimates when the true value of the feature is not known. One such evaluator is *precision*, the ability of a sensor suite to provide repeated estimates that are very close together. It is a function of two sensor attributes: the target location error and the target velocity error. TLE and TVE typically grow with range as indicated in Figure 3. The exact slope of the TLE and TVE lines are a function of the particular sensor being modeled. However, in general, at extreme ranges, the position of targets may not be well known and it may be difficult to distinguish between targets and to count them accurately.

As an example, suppose that a sensor suite reported 27 locations for unit/targets in the AO as depicted in Figure 5. Let's further suppose that through the application of an appropriate cluster algorithm, it is determined that there are really only 4 unit/targets.[11] An *epitome* location is calculated as depicted in the diagram as a consequence of the cluster algorithm.

---

[9] For example, the bivariate normal distribution for target location.

[10] Note that in this discussion we are referring to statistical bias, not operational bias. We assume that the estimates of features have been corrected for operational bias.

[11] Clustering is used when there is no previous information available concerning the disposition of the enemy forces. If there is prior information, then the observations "cluster" around that previous information. For a complete discussion of cluster algorithms, see [16] Duda, and Hart.

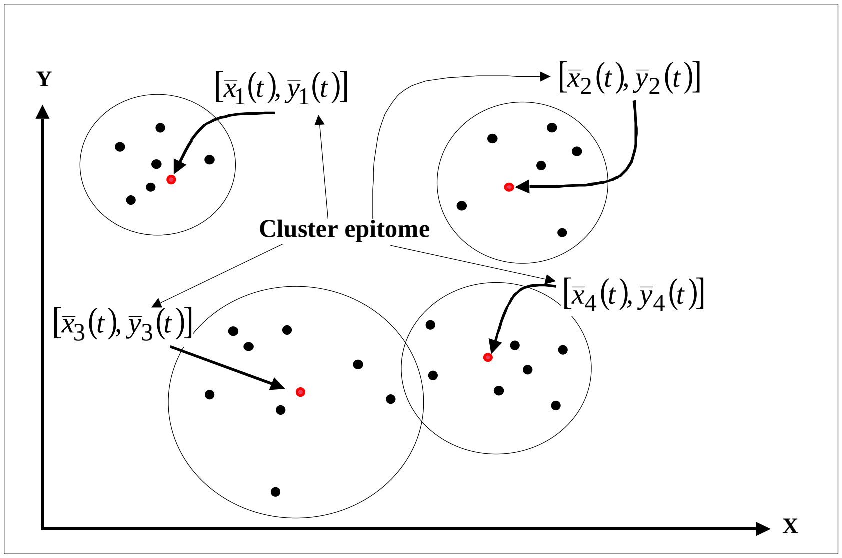

Fig. 5 –Measuring Precision

The cluster epitomes are then the location estimates for the mean of the bivariate normal distributions for the location of each unit/target. For each cluster, we calculate the sample covariance matrix as:

$$\hat{\mathbf{\Sigma}}(t) = \begin{bmatrix} S_x^2(t) & 0 \\ 0 & S_y^2(t) \end{bmatrix} = \frac{1}{n-1}\sum_{i=1}^{n}\left[\mathbf{X}_i(t) - \overline{\mathbf{X}}(t)\right]\left[\mathbf{X}_i(t) - \overline{\mathbf{X}}(t)\right]^T . \quad (1)$$

In this formulation, $\overline{\mathbf{X}}(t) = [\bar{x}(t), \bar{y}(t)]$, the cluster epitome, $\mathbf{X}_i(t) = [x_i(t), y_i(t)]$ are the other cluster locations, and $S_x^2(t)$ and $S_y^2(t)$ are the sample variances. Note that the covariances, $S_{xy}^2(t)$ and $S_{yx}^2(t)$, are taken to be 0. This is justified on the grounds that the vertical and horizontal locations are independent.[12] Precision then is defined to be the determinant of the covariance matrix or $p(t) = \left|\hat{\mathbf{\Sigma}}(t)\right| = S_x^2(t)S_y^2(t)$. Note that this value is always non-negative and a 0 value implies perfect precision. In this case, no true estimate is available and $Q_{cor}\left(\mathbf{F}'(t) \mid \mathbf{F}(t)\right) = \dfrac{p(t)}{\left|\hat{\mathbf{\Sigma}}(t)\right|_{\max}} = \rho(t)$. The practical maximum covariance matrix will be situation dependent.

Measure of Currency: *the latency in completing required sensor operations and local data processing*

In general, the less time required to complete a process the better. Therefore, all of the currency measures compare the time required to perform functions. We distinguish this from the time the process *must* be completed. There are two time metrics associated with this measure.

---

[12] It is also generally the case that $S_x^2(t) = S_y^2(t)$.

These metrics examine the time required to complete the tasks included in the sensor collection process and in pre-fusion data processing:

Metric for Currency (1): the time required to complete target detection and establish a target track.

Metric for Currency (2): the time required to re-task sensors to provide coverage of high priority area targets.

THE FUSION-SUB DOMAIN

The output of the Sensor sub-domain is a series of sensor reports that are forwarded to fusion centers for processing. We assume that reports from like and disparate sensors and sources are combined to produce a COP, $\mathbf{F}^{''}(t)$, that is subsequently disseminated to friendly users in the AO. The level of fusion is not at issue, only the quality of the information produced by the process. The measures of information quality therefore focus on how well this process is accomplished. The correctness and completeness of the process, $Q\left(\mathbf{F}^{''}(t) \mid \mathbf{F}(t), \mathbf{F}^{'}(t)\right)$, however is conditioned on the quality of the information and data received from the sensor suites represented by the quantity, $Q\left(\mathbf{F}^{'}(t)\right)$ in Figure 2.

Fusion

Fusion is the process of combining information from sensors and sources to produce a common, relevant picture of the battlespace. It includes the correlation and analysis of data inputs from a supporting sensor suite. There are essentially two uses of fused information: to nominate targets (target acquisition) and to aid in assessing the enemy's situation and capabilities. Both uses ultimately lead to a decision. In the first case a targeting decision made generally at the tactical level and in the second maneuver decisions at the strategic and operational level of combat.

The first use is generally characterized by automated systems such as the Army's Q-37 Firefinder radar system and sensors that detect mobile missile. The level of fusion in these cases is rather low and is generally completed by the sensor system itself. For example, a moving target indicator (MTI) combines location, speed and direction of movement to help establish a track for the observed target.

Assessing the enemy situation is a more arcane process. It generally consists of both automated and manual processes and is the subject of ongoing resdearch. The level of fusion needed is much higher than that required for target nominations. For example, it may not be sufficient to know where the enemy is, but what he intends to do next or what he is capable of doing next. This level of fusion generally takes place in the command operating center as an adjunct to the intelligence process. However, both distributed and centralized systems are possible.

Completeness

The ultimate goal of the fusion process is to create a picture (COP) of the battlefield that is both complete and accurate. The "picture" consists of a set of identified units or targets whose location is known. The quality of the picture depends upon the completeness and correctness of the entries. The completeness portion of the quality measure then focuses on the number of these targets or units contained in the COP.

Measure for Completeness: *the degree to which detected targets in the AO can be classified*

Used in this context, the term, "classified", means that the detected targets have been described. Some degree of classification can take place at the sensor level. For example, cueing a UAV to fly over a location to view a detection made by JSTARS is an attempt to classify the detected object using a sensor only. Assuming this has been accomplished for one or more of the targets, the chore at the fusion facility is easier, in that the ability to "classify" has been enhanced. Although classification can take place at both the sensor and the fusion facilities, we choose to evaluate its quality at the fusion center.

Fusion Centers

We can again resort to a reliability-type model to analyze the effectiveness of the fusion process and therefore the quality of the information it produces. Fusion is essentially a parallel-sequential processor. Each intelligence discipline (INT) attempts to fuse its internal estimates and forward them to a central fusion processor where fused feature vectors from disparate INTs are then combined to develop the COP. Although this may not be the physical model in all cases, the basic sequence is generally applicable. Figure 5 illustrates the process.

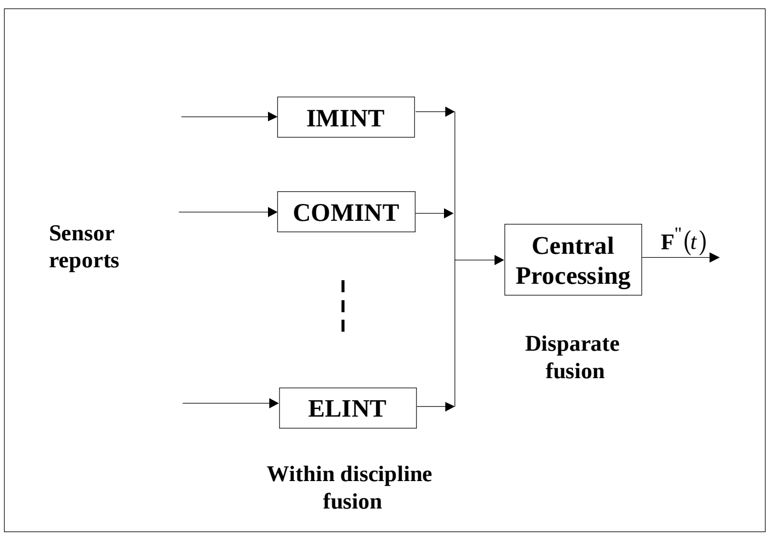

Fig. 5 –Parallel-Sequential Fusion Process

It is reasonable to assume that the longer a fusion facility has to examine the sensor or within discipline reports, the more reliable the results will be. Additional information may be made available and in addition, some time intensive activities such as image processing will improve with more time to process. This also accounts for the time required to retask or cue sensors to focus on targets of interest.

A simple representation of this phenomenon is an increasing exponential. Each of the within-discipline fusion centers and the central fusion center are assigned a time-dependent fraction of detections classified of the form:

$$R_\delta(t) = a + \alpha\left(1 - e^{-\sigma t}\right).$$

The parameter, *a*, represents the fraction of the detected targets that can be fused by the sensors themselves. The sum $0 < a + \alpha \le 1$, is the maximum fraction of the detections capable of being classified at the fusion center and σ is the rate at which detections are classified.

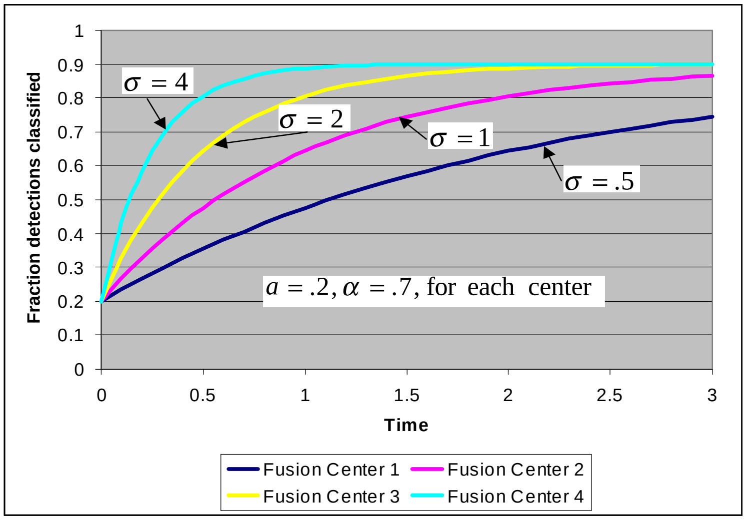

Fig. 6 –Fusion Center Completeness

Several examples are illustrated in Figure 6. For each curve, the parameters a and α are fixed at .2 and .7 respectively and only the rate of classification, σ, changes. Note that in this example, the fraction of classified detections for all centers is bounded between $a = .2$, and $a + \alpha = .9$.

Automation and Control

The rate at which the center classifies detections depends in part upon the degree of automation at the fusion facility. Whereas the minimum fraction of detections that can be classified, *a*, depends upon the characteristics of the sensor suite, the maximum, $a + \alpha$, depends upon the ability of the fusion center to control it.[13] For simplicity, we treat automation as a binary variable: either the facility is automated or it is not. For operational control, we also distinguish two types: dynamic control and static control.

Static Control implies that the fusion facility controls the sensor suite through initial tasking only. A sensor management plan is established at the outset of operations, and it remains fixed. This has the effect of slowing the classification process if the plan was deficient in any way. Therefore, the fraction of classified detections rises slowly over time.

Dynamic Control implies that the fusion center is capable of actively tasking and re-tasking sensors to confirm reports or to bridge gaps in the data. As in static control, the fusion facility begins with a sensor management plan in place. However, in dynamic control, that plan may be altered as the operation progresses. Clearly, this has the effect of rapidly increasing the classification rate.

---

[13] Technically the maximum the facility itself can classify is simply α. The sum however includes the detections that arrive classified.

Combinations of automation and control protocols can produce the type curves depicted in Figure 6. The same should apply to $R_c(t)$, the completeness capability of the central fusion facility in Figure 5. The overall completeness of the fusion process for *k* INT disciplines therefore is:

$$R_f(t) = \left[1 - \prod_{\delta=1}^{k}\left[1 - R_\delta(t)\right]\right] R_c(t).$$

Metric for Completeness: *the estimated reliability of the sensor suite architecture*

The estimated fraction of detected targets classified then is $R_f(t)$ and therefore $Q_{com}\left(\mathbf{F}''(t) \mid \mathbf{F}(t), \mathbf{F}'(t)\right) = R_f(t)$.

Correctness

As in the sensor sub-domain, the appropriate measure of correctness is how close the fused estimate for each unit/target feature is to ground truth. That is, how accurate are the classifications of detections. As before, the problem is assessing how good our estimate and therefore the fusion process is. However, in this sub-domain, we add the additional task of tracking targets from time period to time period. This suggests two measures.

Measure of Correctness (1): *the degree to which the fused target features (classified detections) reflect ground truth*

In addition to developing the COP, the fusion process contributes considerably to reducing uncertainty in the estimates. Therefore, the performance measures that assess the degree to which the fusion process reflects ground truth are the estimate variances. Using the sample variance we can calculate variance estimates for all the features in the feature vectors in $\mathbf{F}''(t)$. We depict this as $\mathbf{S}^2(t) = \left[S_1^2(t), S_2^2(t), \cdots, S_k^2(t)\right]$, where *k* is the number of units/targets classified at time *t*. The metric we seek then is a combination of the elements of $\mathbf{S}^2(t)$.

A weighted average is the obvious choice, except that the elements of $\mathbf{S}^2(t)$ are dimensioned quantities and therefore not directly comparable. One solution is to normalize each entry. This implies that a suitable bound is available for each sample variance. Clearly, 0 is the lower bound for all estimates. The problem is the upper bound. For location for example, the extreme upper bound is the entire AO. However, a more practical figure can be found by examining the operational characteristics of the sensors and sources. Likewise, a reasonable upper bound for speed can be found from the maximum speed of the enemy vehicles. Some features, like direction, have a natural upper bound. The vector of normalized sample variances is then:

$$\mathbf{s}^2(t) = \left[s_1^2(t), s_2^2(t), \cdots, s_k^2(t)\right],$$

where

$$s_i^2(t) = \frac{S_i^2(t)}{S_{i,\max}^2(t)}.$$

The estimate of the quality of the information produced by the fusion process is the weighted average of the elements of $\mathbf{s}^2(t)$:

$$W(t) = \sum_{1=1}^{k} \omega_i s_i^2(t)$$

where $\sum_{i=1}^{k} \omega_i = 1$. This produces a quantity between 0 and 1 where a value close to 0 is desirable. The problem is the basis for selecting the weights. An obvious criterion is the relative importance of the feature in targeting the enemy unit. Using this criterion, the location of the unit/target would be of highest priority.

Metric for Correctness (1): *the weighted norm of the feature estimate variances.*

We have that $Q_{cor,1}\left(\mathbf{F}''(t) \mid \mathbf{F}(t), \mathbf{F}'(t)\right) = W(t)$.

Measure of Correctness (2)*: the degree to which the fusion system maintains the target features (classified detections) over time (tracking)*

The definition of tracking is not confined to correlating moving units/targets. Rather it includes accounting for all units/targets from time period to time period. If *k* targets have been classified at time *t-1* and *n* targets have been classified at time *t*, then we must examine the three cases: $n = k, n < k$ and $n > k$. However, the second case is not possible in that we stipulate that once a unit/target has been classified, it never leaves the set -- only its status changes. Examining the remaining two cases, we have:

a. If $n = k$, then either we are able to correlate the units/targets in $\mathbf{F}''(t-1)$ with the units/targets in $\mathbf{F}''(t)$ units (best case) or we are not able to do so. This produces the 3 cases. Depicted in Figure 7.

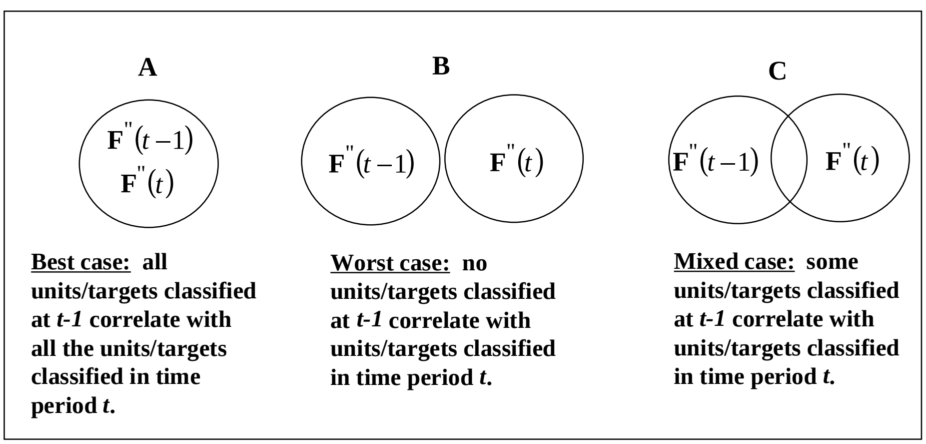

Fig. 7 -Tracking Cases when *n=k*

b. If *n>k*, we have classified more units/targets at time *t* than in time *t-1*. This suggests the three cases depicted in Figure 8

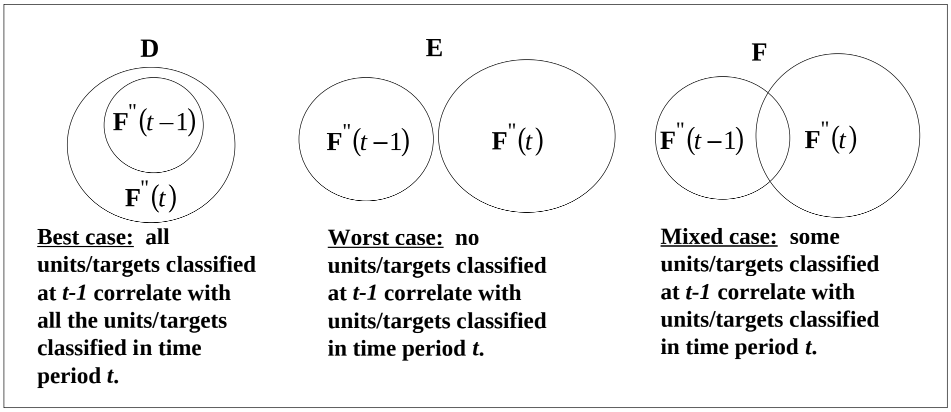

Fig. 8 –Tracking Cases when *n* > *k*

Metric for Correctness (2): *the fraction of units/targets tracked at time t*

The tracking metric from this is calculated as the fraction of units/targets tracked at time *t*, $T(t)$. For cases A and D, $T(t)=1$, for cases B and E, $T(t)=0$, and for cases C and F, $0<T(t)<1$. Therefore we have that $Q_{cor,2}\left(\mathbf{F}''(t)\,|\,\mathbf{F}(t),\mathbf{F}'(t)\right)=T(t)$ and that a composite correctness estimate for the Fusion sub-domain is $Q_{cor}\left(\mathbf{F}''(t)\,|\,\mathbf{F}(t),\mathbf{F}'(t)\right)=\omega W(t)+(1-\omega)T(t)$, where $\omega\in[0,1]$.

CURRENCY

A single time measure is appropriate for the fusion sub-domain.

Measure of Currency: *latency in developing the COP*

The implication is that a shorter time is preferable and therefore the processes used are credited when the they result in a compressed completion time.

Metric for Currency: *the time required to develop the COP using information produced by the integrated multi-sensor suite*

In one sense, there may be tension in this metric and the correctness metric defined above. In the correctness measure, the metric developed improves the sensor suite's score when the time available to complete the fusion is greater – but only up to a point. This metric suggests that the *shorter* time is always valued more.

NETWORK SUB-DOMAIN

In the Network sub-domain, the COP developed in the Fusion sub-domain, $\mathbf{F}''(t)$, is disseminated via a communications network that connects all users to the fusion facilities as depicted in Figure 2. The product received by the users is taken to be the observed COP, $\mathbf{O}(t)$, and it informs both the commander's awareness and the decisions he is to take. The quality of the observed COP, $Q\left(\mathbf{O}(t)\,|\,\mathbf{F}''(t),\mathbf{F}(t),\mathbf{F}'(t)\right)$, is conditioned on the fused information (COP) transmitted from the fusion facilities and is represented by the quantity, $Q\left(\mathbf{F}''(t)\right)$.

COMMUNICATIONS NETWORKS

The battlefield of the future is likely to be highly dispersed and therefore combat will be non-linear. This places considerable demands upon communications networks that support C4ISR functions. For example, is it more efficient to create a single, perhaps out-of-area, fusion center or are distributed centers more efficient? With robust reach-back capability, an argument can be made that considerable efficiencies are possible if we concentrate fusion resources at a single site. But this takes the responsibility for developing the COP out of the hands of the local commander and can easily foster a "not invented here" attitude. Indeed, this occurred during the Kosovo conflict. The Commander of Task Force Hawk rejected the assessment of the Joint Assessment Center at Molesworth England that the threat from the 2nd Yugoslav Army in Montenegro was minimal in favor of his own assessment that they posed a threat to his Apache Helicopters based at Rinas in Albania.[14]

On the other hand, a distributed system has its problems as well. Unevenness in the quality of the fusion process due to widely varying and incomplete resources at some of the sites is clearly a possibility. For example, it is unlikely that sufficient imagery analysts would be available at several sites within a theater to adequately support local commanders. In addition, it is likely that insufficient bandwidth would be made available to all sites to support local fusion. The demands on the communications networks in either case are considerable.

Measure of Completeness: *the degree to which all target features for all classified targets are distributed to all COP users*

Three interpretations are possible. The first is that all users must receive the entire COP. The second is that all users receive some portion of the COP. Finally, the third is that some users receive all of the COP and others only a portion. Note that the case in which some users receive none of the COP is covered as a "zero portion." We further expand on these cases below.

Metric for Completeness: *the likelihood that the user nodes in a network are connected at any time t.*

The completeness metric must reflect the richness of the connectivity within the dissemination network. To illustrate, we postulate a small sub-network consisting of a single fusion center, **F**, three COP users ($U_1, U_2, \text{and } U_3$), and two relay nodes, $T_1 \text{ and } T_2$, (transshipment nodes in the language of network theory). Figure 9 illustrates the connectivity among the nodes. We assume that the network is cyclic. That is, two-way communication is possible on all links. However, we rule out cycles in communicating between nodes.

---

[14] This and other incidents concerning the deployment of Task Force Hawk during Operation Allied Force is documented in [40] Perry, et al.

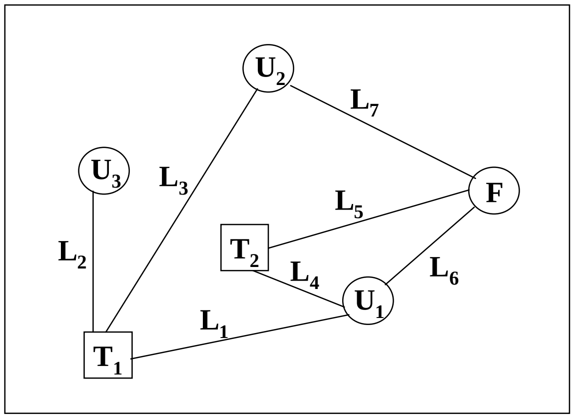

Fig. 9 -Communications Sub-Network

Using a reliability model again, we focus on link (L_i) reliability, $R_i(q)$, where the failure rate function, $r(q)$, is a measure of communications quality and as such is a function of the signal-to-noise ratio (SNR), jamming, bandwidth, etc. Depending upon the convention adopted, we can have $R_i(q)$ increase as q increases or the opposite effect. For example, if $r(q) = q$, then $R_i(q) = e^{-\frac{q^2}{2}}$, and $R_i(q)$ decreases with increasing q. This can be used to model the effects of jamming for example. However, in the case of SNR and bandwidth, we would expect the reliability of the link to increase with increasing values of q. To get this opposite relationship, we can set $R_i(q) = 1 - e^{-\frac{q^2}{2}}$.

The probability that a user is connected then is the probability that at least one path between the fusion facility and the user is available at any time t, given the values of q for each of the links. The information transmitted over the network is then the joint probability that all of the users are connected at time t. For the simple network in Figure 9, we complete the calculations depicted in Table 1. The last column is the probability that the individual user is connected at time t and therefore the assessment of complete network connectivity is the probability that all users are connected or:

$$P_t(N) = \prod_{i=1}^{3} P_t(U_i).$$

Table 1
Network Completeness Assessment

User	Path	Path Reliability	Probability Connected $P_t(U_i)$
U_1	L_6 $L_5 \to L_4$ $L_7 \to L_3 \to L_1$	$R_6(q)$ $R_5(q)R_4(q)$ $R_7(q)R_3(q)R_1(q)$	$1-[1-R_6][1-R_5R_4][1-R_7R_3R_1]$
U_2	L_7 $L_6 \to L_1 \to L_3$ $L_5 \to L_4 \to L_1 \to L_3$	$R_7(q)$ $R_6(q)R_1(q)R_3(q)$ $R_5(q)R_4(q)R_1(q)R_3(q)$	$1-[1-R_7][1-R_6R_1R_3][1-R_5R_4R_1R_3]$
U_3	$L_6 \to L_1 \to L_2$ $L_7 \to L_3 \to L_2$ $L_5 \to L_6 \to L_1 \to L_2$	$R_6(q)R_1(q)R_3(q)$ $R_7(q)R_3(q)R_2(q)$ $R_5(q)R_6(q)R_1(q)R_2(q)$	$1-[1-R_6R_1R_2][1-R_7R_3R_2][1-R_5R_6R_1R_2]$

Although we have been focused primarily on the quality of information disseminated over the network in terms of its completeness, it is also possible to view the combined link probability for each user as the fraction of the COP received by each. For the entire network, the fraction of the COP received by all users is equivalent to the network reliability or $P[\mathbf{F}''(t)] = P_t(N)$. We conclude this because for each user, $P_i[\mathbf{F}''(t)] = P(U_i)$ represents the fraction of the COP received by the user. The product of these probabilities is $P[\mathbf{F}''(t)] = P_t(N)$. This can also be extended to assess the amount of the COP received. The overall average amount of the COP received by all users is $\mathbf{F}''(t)P[\mathbf{F}''(t)]$ and the expected amount delivered to each user is $\mathbf{F}''(t)P_i[\mathbf{F}''(t)]$. This formulation can lead to an assessment of the amount of information that is common among all users and the amount that can be shared.

Shared Information

Figure 10 is a collapsed depiction of Figure 9 that focuses on the amount of information received by the users. The shaded circles in the diagram represent the amount of information (portion of the COP) received by each of the three users in Figure 9. The white circles represent the entire COP. The fraction of the COP represented by the shaded circles is $P_i[\mathbf{F}''(t)]$ on the arcs emanating from the fusion center. The small area in the center of the three joined circles represents the information that is common among all the users whereas the residual gray area has the potential to be shared among all the users depending upon the ability of the group to collaborate. It is clear that the ability to collaborate has the potential to increase the amount of information shared among the users thus contributing to shared situational awareness.

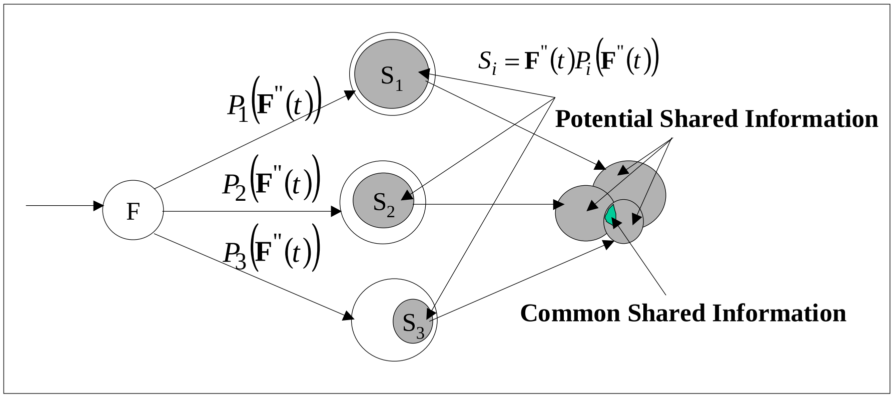

Fig. 10 –Shared and Common Information

Functional Interpretations

Finally, we address the three interpretations suggested by the completeness measure. We first note that $P_t(N)$ can be interpreted as "the fraction of the COP received by all users", or "the fraction of the users receiving all of the COP." Thus we account for the first two interpretations. The third is a bit more problematic. Suppose each user required information only on those targets/units within its area of operations and that only this portion of the COP is to be disseminated to each. This is particularly applicable to the non-linear battlefield. This could be interpreted then as each requiring a fraction, φ_i, of the COP, $\mathbf{F}''(t)$. The combined link probability for each user then would represent the probability that the user received the portion of the COP represented by $\varphi_i \mathbf{F}''(t)$. The network completeness score, $P_t(N)$, would then represent the probability that each user received the fraction of the COP it required.

Based on the foregoing, the completeness metric for the Network sub-domain is $Q_{com}(\mathbf{O}(t) \mid \mathbf{F}''(t), \mathbf{F}(t), \mathbf{F}'(t)) = P_t(N)$.

Measure of Correctness: *the degree to which the COP users receive the distributed information (COP) without degradation*

Network correctness is measured in terms of the likelihood that all users receive the same COP or portion of the COP that was transmitted to each from the fusion facilities. This is essentially the probability of correct message receipt (PCMR) for the entire communications network used to disseminate the COP to users.

Metric for Correctness: *probability of correct message receipt (PCMR)*

The conditional probability, $P_{ij}(\mathbf{O}(t) \mid \mathbf{F}''(t))$, is defined as the probability that, at time *t*, the user U_i receives the observed COP, $\mathbf{O}(t)$, given that the COP, $\varphi_{ij}\mathbf{F}''(t)$ was transmitted to user U_i from the fusion facility *j*.[15] These probabilities are related to the quality of the channel(s) over which the information is transmitted. Therefore, such things as SNR, bandwidth

---

[15] For the rest of this discussion, we assume that $\varphi_{ij} = 1$. That is, we assume that interpretations 1 and 2 apply. Either all users receive a fraction of the entire COP or the entire COP is received by a fraction of the users.

and jamming are also determinants of the PCMR. However, it is also dependent upon the input to the channels. The PCMR then is the joint probability that the COP was transmitted correctly from fusion facility *j* and that the user U_i received the observed COP correctly or

$$P_{ij}\left(\mathbf{O}(t),\mathbf{F}''(t)\right)=P_j\left(\mathbf{F}''(t)\right)P_i\left(\mathbf{O}(t)\,|\,\mathbf{F}''(t)\right).$$[16]

The problem then is to find adequate representations for the marginal probabilities, $P_j\left(\mathbf{F}''(t)\right)$, and the conditional probabilities $P_{ij}\left(\mathbf{O}(t)\,|\,\mathbf{F}''(t)\right)$. The second of these is totally dependent upon the reliability of the communication paths between the fusion facility *j* and the user U_i. This is the connectivity probability calculated above in Table 1, or $P_t(U_i)$. Recall that this quantity is developed from the individual link reliabilities with the parameter *q* representing the SNR, jamming, bandwidth, etc. The marginal probability, $P_j\left(\mathbf{F}''(t)\right)$, is the probability that the COP, $\mathbf{F}''(t)$, will be transmitted correctly and is therefore a function of the communications equipment and personnel within the fusion facility. These probabilities should be assessed empirically by examining performance in deployments and exercises and simulations. The PCMR at time *t* for user U_i therefore is now:

$$\mathrm{PCMR}_{ij}=P_{ij}\left(\mathbf{O}(t),\mathbf{F}''(t)\right)=P_j\left(\mathbf{F}''(t)\right)P_t(U_i).$$

The overall network PCMR is the joint probability of all the fusion facility-to-user PCMRs or:

$$\mathrm{PCMR}_t=\prod_{j=1}^{n}\prod_{i=1}^{m}P_j\left(\mathbf{F}''(t)\right)P_t(U_i).$$

This is equivalent to the average fraction of the observed COP that is correctly received by each user. Therefore the correctness metric for the Network sub-domain is $Q_{cor}\left(\mathbf{O}(t)\,|\,\mathbf{F}''(t),\mathbf{F}(t),\mathbf{F}'(t)\right)=PCMR_t$.

Measure of Currency: *transmission latency from fusion facility to user*

Currency in a network is dependent upon the rate at which data can be transmitted over the network's links. This is dependent upon bandwidth and the complexity of the communications paths between subscribers. It is generally considered advantageous for this time to be minimum.

Metric for Currency: *the average end-to-end time delay for transmitting the COP from the fusion facilities to the users*

There are several possible conventions for calculating the time delay from a single fusion facility to a specific user. A conservative approach is to calculate the time required along the "longest" path. Another is to select the minimum and another might be to calculate the average of all paths. Once the individual fusion facility to user time delays have been calculated, the overall average network transmission delay is simply the average of these times.

---

[16] See for example, [6] Blahut.

A Note on the General Applicability of Network Metrics

As mentioned earlier, network metrics reflect the richness of the connectivity within the network. The simple example presented here illustrates a rather weak network. In most cases, terminal nodes may also be relays thus providing considerably more alternative paths. In the limit, every node is a relay and every entity on the battlefield is a node. The Army refers to this as a “nodeless network”, the idea being that with such a richly connected network the loss of a node will not degrade performance in any appreciable way ([30] Nichols). In fact, if the network is a complete graph with *n* vertices, there are $\binom{n}{2} = \frac{n(n+1)}{2}$ edges. A complete graph is one in which distinct vertices are connected by an edge. With 10 nodes or vertices for example, we have 45 binary connections and for 100, we have 4,950.[17]

With robust networks of this type, it is perhaps unnecessary to calculate the likelihood that all users receive the COP. Given that there is likely to be several originating “fusion facilities”, the task of enumerating each path is formidable indeed. The problem of correct message receipt is also improved.

The problem however will be in estimating the conditional probability $P_{ij}\left(\mathbf{O}(t)\,|\,\mathbf{F}''(t)\right)$. This value is clearly dependent upon the redundancy of paths between the fusion center and the users and therefore the number and length of those paths becomes an important factor. One way to estimate this quantity is to calculate the longest path between the fusion center and the user (in terms of the number of edges or links traversed). For a fully connected network (complete graph), the longest path is $n-1$ where *n* is the number of nodes or vertices. The problem is calculating the number of such paths in the network. For example, for a three-node network, there is only one 2-link path from any one node to another. For a four-node network the number of three-link paths is 2 but for a five-node network, the number of four-link paths is 6. There are several ways one might approximate the number. One might be to assume there are *n* paths of size $n-1$. If we let *p* be the conditional probability for one $n-1$ link, then we might assess the overall conditional probability to be $P_{ij}\left(\mathbf{P}(t)\,|\,\mathbf{F}''(t)\right) = 1-(1-p)^n$.

THE COGNITIVE DOMAIN

The product produced in the information domain is the observed common operating picture depicted as the feature vector, $\mathbf{O}(t)$. In the Cognitive Domain, the products of the information domain are used to take decisions. The mental processes that transform $\mathbf{O}(t)$ into a decision and a subsequent action are not well understood. They depend upon a range of factors including a few psychological concepts. The focus here is on the steps taken before decision and subsequent action take place. The cognitive process is described for individuals and for interacting, collaborating individuals. The objective is to identify the factors that most influence variations in individual situational awareness, collaboration, and shared situational awareness, prior to decision making.

---

[17] See for example [22] Jackson and Thoro.

Awareness, situational awareness, shared situational awareness, and collaboration are terms frequently encountered in discussions of combat decision making. Formal definitions of these terms exist, but they are not always consistent and sometimes they are not precise enough to satisfy the requirements of rigorous mathematical analysis. Below, we offer definitions of these terms that are used in this research.

Def. 4: *Awareness* is the generic ability to draw inferences from the observed COP generated in the information domain.

Def. 5: *Situational awareness* is the ability of a decision maker to draw inferences about the situation facing him based on the observed COP. [18]

Def. 6: *Shared situational awareness* is the ability of a decision making team to share inferences about the current situation.[19]

Def. 7: *Collaboration* is a process in which two or more people work together to achieve a common objective.

The decision maker must *understand* the picture presented to him, that is, he must be *aware* of what he sees and hears. There is no guarantee that the commander will be *cognizant* of the situation presented to him and therefore there is no guarantee that he will be willing to act regardless of how complete, correct, and timely the COP is. His actions will depend upon the situation, his skills, and the collaborative environment. In general, however, the information he needs must be of sufficient quality to make him fully aware of the situation before him. Consequently, it is important to develop a functional relationship between the various quality metrics and awareness.

Realizing the complexity of representing the functional relational relationships between the various quality metrics and awareness, we choose to address them in three steps: (1) first model an individual decision maker's situational awareness, (2) next, model the information available to individuals participating together in some joint collaborative action; and (3) finally, modify the model of an individual's situational awareness to include factors representing information available to collaborating individuals, then extend this model to that of the situational awareness of an entire collaborating team

INDIVIDUAL SITUATIONAL AWARENESS

The task of identifying what it will take for a decision maker to correctly assess the situation presented to him, i.e., "be aware", is a complex business. Several factors come into play: education and training, experience, the current situation, cultural background, personality,

---

[18] Other definitions of situational awareness focus more on a state of mind rather than the ability to infer. Carl Builder referred to situational awareness as a state attained by a decision maker in which he is cognizant of the key physical, geographical, and meteorological features of the battlespace that will enable his command concept to be realized ([10] Builder, Bankes and Oxley pp xv).

[19] The Army's Digitization Office defines shared situational awareness as "…the ability of a unit to know where its friends are located, where the enemy is, and to share that information with other friends, both horizontally and vertically, in near real-time." Again, this is a state focused definition. It describes the state required to achieve shared situational awareness. We prefer to use the more useful inference definition ([41] U.S. Army Digitization Office).

language, the opportunity to collaborate with others, the *quality of the information* presented, etc. We propose the following metric for individual situational awareness:

Metric for Degree of Individual Situational Awareness: The fraction of fused feature vectors that can be interpreted by the decision maker.

This emphasizes the use of the individual components of the COP and includes a reference to the ability of the individual decision maker. It also does not place greater or lesser value on the correct interpretation of fused feature vectors by the decision maker: rather it focuses exclusively on the ability of the decision maker to interpret what he sees.

It is impossible to deal with all of the factors that contribute to an individual decision maker's level of situational awareness. Instead, we resort to an agent representation of a decision maker. That is, some combination of the factors listed in the previous paragraph will predispose the commander to quickly grasp the situation and others that will not. We simply posit a continuum and select discrete points on that continuum. For example, suppose we focus on three factors: education and training, experience, and the current situation. For all of these factors, the domain is clearly continuous. Rather than deal with the complexities of continuous domains, we instead define two discrete points for each as depicted in Table 2.

Table 2
Exemplar Discrete Awareness Attributes

Attribute	**High**	**Low**
Education and Training	Graduate of advanced service and civilian schools	Limited education beyond undergraduate studies and basic service school
Experience	Senior officer who has commanded troops in several operations.	Junior officer with limited combat experience.
Current situation	Familiar with the current situation.	Unfamiliar with the current situation.

A strict combinatorial assessment produces eight distinct possible awareness conditions that characterize a commander's predisposition to grasp the situation presented to him. We refer to these as *decision agents*. Suppose we focus on just four that descend in the order of awareness of the situation presented. These are described in Table 3 where the exemplar decision agents are denoted by $\mathbf{\Phi}_i$.

Table 3
Exemplar Decision Agents

$\mathbf{\Phi}_i$	**Agent Characterization**	**Description**
$\mathbf{\Phi}_1$	Highly capable	An experienced, well educated commander familiar with the situation confronting him and a veteran of considerable field training.
$\mathbf{\Phi}_2$	Diminished capability	An experienced commander with limited education, unfamiliar with the situation confronting him and with some field training.
$\mathbf{\Phi}_3$	Marginally capable	An inexperienced commander with limited education, unfamiliar with the situation confronting him but with some field training..
$\mathbf{\Phi}_4$	Incapable	An inexperienced commander with limited education, unfamiliar with the situation confronting him and with little field training.

Next, we let $A \in [0,1]$ represent the degree (level) of individual situational awareness each of the commander decision agent types possesses. For example, a commander who is totally aware of the situation presented to him, that is, one who is able to interpret almost the entire observed COP, has a score close to 1. The remaining question is how does the quality of the information represented in the COP influence the commander's awareness? It seems reasonable to assume that information of higher quality will tend to increase awareness regardless of the commander's inherent awareness characterization. Consequently, we seek a functional relationship in which the dependent variable is "awareness", *A*, and independent variables are information quality measures.

The chore remaining is to relate the awareness of the four alternative decision agents to each of the total information quality measures. This suggests four iso-relationships for each of the measures. Recall that the awareness range (the dependent variable) is $A \in [0,1]$. For completeness and correctness, the domain is also between 0 and 1. What is needed is a relationship that shows decision agents with high awareness ($\mathbf{\Phi}_1$ and $\mathbf{\Phi}_2$) becoming more situationally aware with increasing completeness and correctness, and the converse for decision agents with low awareness ($\mathbf{\Phi}_3$ and $\mathbf{\Phi}_4$). The so-called logistic or S-curve depicted in Figure 3 illustrates such a relationship for completeness. For low levels of information quality, awareness is at its lowest level. For some region of awareness above this threshold, awareness increases rapidly tapering off considerably beyond this region. These curves are all of the form:

$$1. \quad A_{\Phi_i} = \frac{e^{\beta_0 + \beta_1(\Phi_i)C}}{1 + e^{\beta_0 + \beta_1(\Phi_i)C}}.$$ [20]

Equation 1 utilizes parameter *C* to represent information completeness. Parameters β_0 and $\beta_1(\Phi_i)$ reflect the decision agent's characterization.

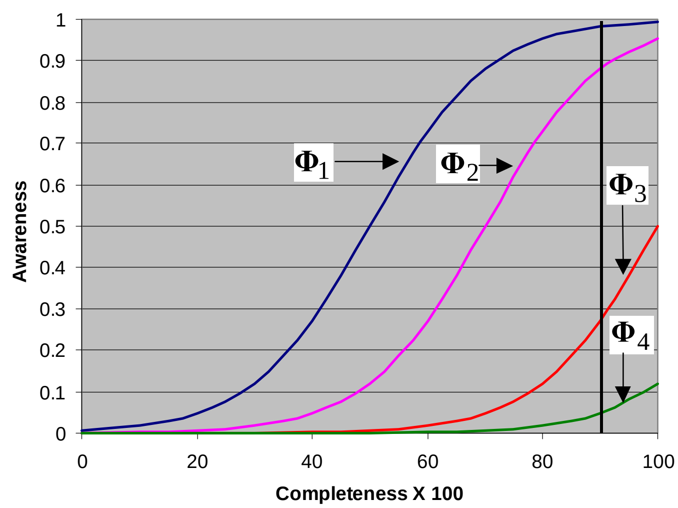

Fig. 10.3 – S-Curve Representation of Quality Effects on Awareness

---

[20] This curve is sometimes referred to as the *logistics response function* or the *growth curve*. See [29] Neter and Wasserman.

The relationship defined in Equation 1 is more generally applicable to quality of information. Extending Equation 10.1, the general relationship is:

$$2 \quad A_{\Phi_i}(t) = \frac{e^{\beta_0 + \beta_1(\Phi_i)Q(\mathbf{O}(t))}}{1 + e^{\beta_0 + \beta_1(\Phi_i)Q(\mathbf{O}(t))}},$$

where $Q(\mathbf{O}(t))$ is the quality of the observed COP at time *t*. We interpret $A_{\Phi_i}(t)$ as the Degree of Situational Awareness -- the fraction of the observed COP that an individual decision maker with ability $\mathbf{\Phi}_i$ can interpret at time *t*. This function is related to time through the quality measure, $Q(\mathbf{O}(t))$. It is parametrically related to $\mathbf{\Phi}_i$ in that we postulate a finite set of capabilities and adjust $\beta_1(\Phi_i)$ accordingly.

This relationship must now be refined to account for the effects of individuals participating in some joint action prior to decision making. That is, we wish to explicitly represent the effects of collaboration on the individual decision maker as the first step toward measuring shared situational awareness for a collective decision team.

SHARED SITUATIONAL AWARENESS

Our model of individual situational awareness thus far includes parameters representing differences among individual decision agents, β_0 and $\beta_1(\Phi_i)$, and the quality of information produced in the Information Domain, $Q(\mathbf{O}(t))$. To describe shared situational awareness we must augment the current model with parameters representing the complex interactions in situations involving more than one individual that may result in *shared situational awareness*. We propose the following metric:

Metric for Degree of Shared Situational Awareness: The fraction of fused feature vectors in the COP that can be interpreted in a similar way by members of a team, whether or not they collaborate.

This emphasizes the importance of individual situational awareness and allows consensus to exist even though individual decision makers have not collaborated. Collaboration may not be needed when information quality is very good, each of the commander agents is highly capable and know that the other commander agents are of similarly capable, and the situation at hand is not unusual or complex. It also emphasizes the importance of the factors affecting individual situational awareness, the quality of collaboration, the impact of collaboration upon individual decision agents, and factors representing situation complexity. The focus here will be on the quality of collaboration and the impact of collaboration upon individual decision agents.

Collaborating Teams

There are two significant categories of attributes affecting collaborating teams: individual and group.

(1) **Individual:** Experience; familiarity with situations similar to the current situation; ability to share knowledge; ability to access other's knowledge; access rights; authority level; and collaboration tool competence.

(2) **Group:** Task structure; role specification; shared operational model; degree of common language; group dynamics; and quality of interoperability provided by the collaboration environment.

Both are important to describing a collaboration, and therefore both are considered in modeling shared situational awareness. Of concern however, is identifying the factors that impact interactions among collaborators and selecting those that have the most impact. The literature seems to suggest that formality of interaction, group size, group roles, and task complexity are the most important. The structural model we propose for collaborative team interaction is derived from these attributes and factors.

Transactive Memory Systems

Information can be stored and retrieved internally by an individual. However, if an individual stores information externally, the storage and retrieval process must also include the location of the information. If externally stored information resides in another person, a *transactive memory* system exists. Individuals can be assigned as information stores because of their personal expertise or through circumstantial knowledge responsibility.

The term "transactive" is used with memory system because of the nature of the process involved and its role in collaborative decision making. Participants in the system conduct transactions concerning the shared information COP based on what portion of it each has received. In a well-ordered and experienced team, individuals need only store what is unique to their role and depend upon others to do the same. An individual member therefore needs to know who has what information or who knows who has what information. A fully matured team therefore is based on some degree of trust as well as experience.

A Model for Developing a Transactive Memory System

Ulhoi and Gattiker define an iterative process for the incremental divergence or convergence of knowledge in a description of how people develop a conceptual framework for solving a technological problem ([48] Ulhoi and Gattiker pp 7-87 – 7-93). The key features are the iterative stages of individual information assessment, followed by team discussion, leading to some state of shared situational awareness. The team discussion period consists of reinforcing and refuting current beliefs about the situation. Knowledge divergence results from the presentation of interpretations from collaboration team members. Knowledge convergence is the result of consensus derived from assessment about the beliefs of other team members during the team's discussions. There are three shared situational awareness states in this process:

(1) In the *Initial Calibration* state, team members have achieved consensus about what roles each team member can and will perform in the collaboration and the team generates initial alternative actions for further discussion.

(2) In the *Structured Knowledge* state, team members begin to organize internally and externally stored information for the situation and begin to form transactive memory. The team has progressed to consensus about who knows what about the situation and has identified alternatives for further analysis and comparison.

(3) In the final state, *Common Knowledge*, not only do team members reach consensus about who believes what but also about what is true for the situation. Alternatives proposed are assessed against the consensus reached about who knows what, and what is true.

Estimating Team Hardness

A functional model has been selected for *team hardness*, the degree to which the collaborating team achieves effective performance. A basic assumption is that the rate at which the ratio of shared information storage or complexity in the transactive memory grows is linear. The rate depends upon the degree of consistency maintained by team membership over time and by the complexity of the situation. We represent the growth rate as a parameter, *k*, expressed in units of hardness per unit time. With a constant growth rate model, we can represent team hardness as a simple increasing exponential. If we let *t* represent the time elapsed since the start of the operation (usually in minutes), and τ the length of time the team has been training or operating together (usually in months), transactive memory is $TM(T)=1-e^{-kT}$, where $T=\tau+t$. The operation is assumed to have begun at time $t=0$.

The Extended Model

The mathematical model for shared situational awareness extends equation 2 to account for team the collaboration group attributes discussed above. The individual is placed in a team and his situational awareness is measured in that setting. Note that this is not the same as team awareness but rather the effect of team dynamics on an individual member of a collaborative decision making process. The contribution is derivative of the transactional memory function and therefore, team hardness. Next, we address consensus that develops among collaborating individuals and its impact on the team's shared situational awareness. Finally, we account for diversity of decision agent capabilities among the collaborators that results in our composite model for the degree of shared situational awareness.

Team participation can have both a salutary effect and a deleterious effect on individual awareness. Presumably team participation produces positive synergies that improve individual performance. However, there can be instances where individual team members with limited ability but with positions of authority enforce their will on the process to the detriment of other individuals in the team. In addition, quality, $Q(\mathbf{O}(t))$, may decrease over time based on the fusion sub-domain metrics. This effect is included in the individual shared awareness function, expressed in Equation 2. A new measure of individual situational awareness that combines these factors and that includes transactive memory is:

$$3 \quad A'_{\Phi_i}(t)=\frac{e^{\beta_0+\beta_1(\Phi_i)[Q(\mathbf{O}(t))+TM(T)]}}{1+e^{\beta_0+\beta_1(\Phi_i)[Q(\mathbf{O}(t))+TM(T)]}}.$$

Note that if $\beta_0\to-\infty$ at time $t=0$, $Q(\mathbf{O}(t))=0$ and $TM(T)=TM(\tau)=0$ for a team with no collective experience. $A'_{\Phi_i}(t)$ is now the fraction of the observed feature vectors interpreted by the individual decision maker with capability Φ_i and with benefit of team participation.

The next step is to evaluate the situational awareness of the team when working together. This is what we refer to as *shared situational awareness*. We now wish to assess the collective fraction of the observed COP, $\mathbf{O}(t)$, that can be interpreted by the entire team. This will be a function of the individual situational awareness of the members with different capabilities when working in the team environment and their situational awareness of the individual feature vectors in the observed COP. This is a bit more problematic. For any two team members for example, we wish to know which feature vectors they can jointly interpret. This implies that we not only know the fraction of the observed COP they can interpret, but WHICH features they can interpret.

Suppose we let *m* be the number of feature vectors in the observed COP, i.e., the cardinality of the set $\mathbf{O}(t)$ is *m* or $\|\mathbf{O}(t)\| = m$, and the number of feature vectors interpreted by all team members with capability Φ_i at time *t* is $mA'_{\Phi_i}(t)$. However, the feature vectors interpreted may not be the same for each individual. For team member *j* with capability Φ_i, the cardinality of the set of feature vectors he can interpret is therefore $\|\mathbf{F}_{j\Phi_i}(t)\| = mA'_{\Phi_i}(t)$. Since it is impossible to know which vectors have been interpreted, we examine instead the possible overlaps. The intersection set between two team members, *j* and *k*, one with capability Φ_i, and one with capability Φ_l is given by: $\mathbf{F}_{j\Phi_i}(t) \cap \mathbf{F}_{k\Phi_l}(t)$. The smallest number of element in this set (overlap) is $\left|A'_{\Phi_i}(t) - A'_{\Phi_k}\right| m$ and the largest it can be is $\min\left\{mA'_{\Phi_i}(t), mA'_{\Phi_k}(t)\right\}$. A reasonable estimate therefore of the fraction of overlapping feature vectors interpreted by team members *j* and *k* with capabilities Φ_i and Φ_l is the average of these two quantities or:

$$4 \quad G_{jk}(t) = \frac{1}{2}\left[\left|A'_{\Phi_i}(t) - A'_{\Phi_l}(t)\right| + \min\left\{A'_{\Phi_i}(t), A'_{\Phi_l}(t)\right\}\right].$$

For example, if $i = l$, $G_{ik}(t) = (1/2)A'_{\Phi_i}(t)$. This appears to be right in that on average, two team members that can interpret the same number of feature vectors will, on average, have half in common.

Next we need to account for the composition of the team itself. That is, we must account for the number of each capability type present in the team and the size of the team. To do this for each feature vector, we pair all possible capability types making the calculation above and averaging the result, or, for a team of size *n*:

$$TA(t) \approx 1/\binom{n}{2} \sum_{j=1}^{n-1} \sum_{k=j+1}^{n} G_{jk}(t).$$

The degree of shared situational awareness, *TA*(*t*), is the collection of fused feature vectors at time *t* that can be interpreted in a similar way by members of a team if they collaborate. With this equation, we achieve the desired result: the development of a metric that assesses the effects of quality information processing, individual situational awareness and team collaboration on shared situational awareness.

SUMMARY OF MEASURES AND METRICS

We have developed a framework for developing quantitative metrics for the quality of information and we have suggested several mathematical representations. In addition, we have mathematically linked the quality of information to shared situational awareness and in the process, suggested how collaboration and team hardening contribute. The following summarizes both the methodology developed and the suggested mathematical expressions in both the information and cognitive domains.

In formation Domain

We have argued that the information quality metrics of correctness and completeness can be treated as probabilities and hence conditional and joint probability calculations applied. As currently formulated, this is not exactly correct because, among other things, $\mathbf{F}(t)$, $\mathbf{F}^{'}(t)$, $\mathbf{F}^{''}(t)$ and $\mathbf{O}(t)$ are not random variables and therefore $Q(\mathbf{F}(t))$, $Q(\mathbf{F}(t),\mathbf{F}^{'}(t))$, $Q(\mathbf{F}(t),\mathbf{F}^{'}(t),\mathbf{F}^{''}(t))$ and $Q(\mathbf{F}(t),\mathbf{F}^{'}(t),\mathbf{F}^{''}(t),\mathbf{O}(t))$ are not probabilities. The composite completeness and correctness, that is, the overall quality of the information produced by the C4ISR system, however can be calculated in the same way that a chained conditional probability is calculated. For correctness and completeness, we have that the composite calculation is:

$$\begin{aligned} Q(\mathbf{O}(t),\mathbf{F}(t),\mathbf{F}^{'}(t),\mathbf{F}^{''}(t)) &= Q(\mathbf{O}(t) \mid \mathbf{F}(t),\mathbf{F}^{'}(t)\mathbf{F}^{''}(t))Q(\mathbf{F}(t),\mathbf{F}^{'}(t)\mathbf{F}^{''}(t)) \\ &= Q(\mathbf{O}(t) \mid \mathbf{F}(t),\mathbf{F}^{'}(t)\mathbf{F}^{''}(t))Q(\mathbf{F}^{''}(t) \mid \mathbf{F}(t),\mathbf{F}^{'}(t))Q(\mathbf{F}(t),\mathbf{F}^{'}(t)) \\ &= Q(\mathbf{O}(t) \mid \mathbf{F}(t),\mathbf{F}^{'}(t)\mathbf{F}^{''}(t))Q(\mathbf{F}^{''}(t) \mid \mathbf{F}(t),\mathbf{F}^{'}(t))Q(\mathbf{F}^{'}(t) \mid \mathbf{F}(t))Q(\mathbf{F}(t)). \end{aligned}$$

The chained calculation for completeness and correctness using the metrics defined in earlier and summarized in Table 5 are:

$$Q_{com}(\mathbf{O}(t),\mathbf{F}(t),\mathbf{F}^{'}(t)\mathbf{F}^{''}(t)) = R(d)R_f(t)P_t(N) \text{ and}$$

$$Q_{cor}(\mathbf{O}(t),\mathbf{F}(t),\mathbf{F}^{'}(t)\mathbf{F}^{''}(t)) = \rho(t)[\omega W(t) + (1-\omega)T(t)]PCMR_t.$$[21]

Table 4
Summary of Information Domain Measures

Sensor Measures	Fusion Measures	Network Measures
Completeness: The degree to which the information received and transmitted is free of gaps.		
The degree to which real targets in the area covered are detected.	The degree to which detected targets in the AO can be classified.	The degree to which all target features for all classified targets are distributed to all COP users.
Correctness: The degree to which the information agrees with ground truth.		
The degree to which the true target features approximate their ground truth values.	The degree to which the fused target features (classified detections) reflect ground truth. The degree to which the fusion system maintains the target features over time (tracking).	The degree to which the COP users receive the distributed information (COP) without degradation.
Currency: The time required for the ISR system and the fusion process to produce a common operating picture of the combat situation.		
The latency in completing required sensor operations and local data processing.	Latency in developing the COP.	Transmission latency from fusion facility to user.

[21] This assumes that precision is used as a measure of sensor correctness.

Table 5
Summary of Information Domain Metrics

Measure	**Sensor**	**Fusion**	**Network**
Completeness	$R_t(d)$: The percentage of targets detected.	$R_f(t)$: The percentage of detected targets identified.	$P_t(N)$: The fraction of unit/target features for all classified units/targets that are distributed to all COP users.
Correctness	$\alpha(t)$: The fractional bias in the estimate. $\rho(t)$: The fractional precision.	$W(t)$: The degree to which detected targets reflect ground truth. $T(t)$: The degree to which the fusion system maintains the target features over time (tracking).	PCMR_t : The fraction of the distributed COP received by the users without degradation.
Timeliness	t_1 : Time required to complete target detection and establish a target track. t_2 : The time required to retask sensors to provide coverage of high priority area targets.	t_3 : The time required to develop the COP using information produced by the integrated multi-sensor suite.	t_4 : The average end-to-end time delay for transmitting the COP from the fusion facilities to the users.

Cognitive Domain

The link between the information domain and the cognitive domain is through the ultimate measure of information quality, $Q(\mathbf{O}(t))$. The development of this link is summarized below.

We begin with a measure of individual situational awareness, $A_{\Phi_i}(t)$, based on certain capability characteristics of the decision maker. Next, we assess the effects of team participation through collaboration on shared situational awareness. The effects of team participation depends upon the level of team hardness achieved which ultimately influences the quality of the transactive memory system, $TM(T)$, shared by the team. The result is a mathematical expression for shared situational awareness for team members with inherent capability characteristics, $\mathbf{\Phi}_i$:

$$A'_{\Phi_i}(t) = \frac{e^{\beta_0+\beta_1(\Phi_i)[Q(\mathbf{O}(t))+TM(T)]}}{1+e^{\beta_0+\beta_1(\Phi_i)[Q(\mathbf{O}(t))+TM(T)]}}.$$

Next, we assess the pairwise interactions of the team members with different (or similar) capability characteristics:

$$G_{jk}(t) = \frac{1}{2}\left[\left|A'_{\Phi_i}(t) - A'_{\Phi_l}(t)\right| + \min\left\{A'_{\Phi_i}(t), A'_{\Phi_l}(t)\right\}\right].$$

Finally we account for the composition of the team itself too include the number of team members and the capabilities of each. This results in the approximate relationship for a team of size n:

$$TA(t) \approx 1/\binom{n}{2}\sum_{j=1}^{n-1}\sum_{k=j+1}^{n} G_{jk}(t).$$

The degree of shared situational awareness, $TA(t)$, is the collection of fused feature vectors at time t that can be interpreted in a similar way by members of a team if they collaborate. With this equation, we achieve the desired result.

CONCLUSIONS

We firmly believe that to adequately assess the contribution of C4ISR toward achieving a network centric warfare capability a new set of mathematically rigorous concepts and tools are required as is the case with the development of any new branch of science. This work represents a small step toward doing this by solidifying and *quantifying* some information superiority concepts that up to this point have been abstract or vague. The focus has been on both the quality of information processing and some of the cognitive aspects of achieving individual and shared situational awareness. However, this is not the end of the story. Much still needs to be done:

In some cases, data may exist in the military C4ISR community to confirm or disconfirm the mathematical relations presented here. In these cases, locating and assessing the data is required. Where data does not exist, further experimentation or historical analysis is required. Although we are confident that the methodology is workable, we are less certain about the mathematical formulations. This needs to be verified experimentally, if possible.

As noted earlier, the discussion of the Cognitive Domain is not complete. The relationship between information quality and shared situational awareness is the first step in the decision making process. Further work is needed to codify the relationship between shared situational awareness and the ability of the decision maker to make inferences from the COP, that is his understanding of the situation.

REFERENCES

1. Alberts, D.S., Garstka, J. J., and Stein, F. P., *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2ed., the DoD C4ISR Cooperative Research Program, 2000.

2. Allard, C. K., Command, Control, and the Common Defense, Yale Press, New Haven, 1990.

3. Askins, Scott W., *The Black Box Conundrum of Network Centric Warfare*, Thesis, Naval War College, Newport, Rhode Island, 2000.

4. Ayyub, B. and McCuen, R., Probability, Statistics and Reliability for Engineers, CRC Press, 1997.

5. Bandura, Albert, *Self-Efficacy: The Exercise of Control*, New York: W.H. Freeman and Company, 1997.

6. Blahut, R. E., Principles and Practice of Information Theory, Addison-Wesley, 1988.

7. Blake, I. F., An Introduction to Applied Probability, Krieger, 1987.

8. Bowerman, B. and O'Connell, R., *Linear Statistical Models: An Applied Approach (Second Edition)*, Boston: PWS-Kent Publishing Co., 1990.

9. Brown, S. M., Santos, E., Jr., Banks, S., and Oxley, M., "Using Explicit Requirements and Metrics for Interface Agent User Model Correction," *Proceedings of the Second International Conference on Autonomous Agents*, Minneapolis, United States, May 10-13, 1998, pp. 1-7.

10. Builder, C. H., Bankes, S., and Nordin, R., *Command Concepts: A Theory Derived from the Practice of Command and Control*, Santa Monica, Calif.: RAND, MR-75-OSD, 1999.

11. Clark, H. H., *Using Language*, New York: Cambridge University Press, 1996.

12. Clark, H. H. and Brennan, S. E., "Grounding in Communication" in Resnick, L.B., Levine, John M., and Teasley, S.D., ed., *Perspectives on Socially Shared Cognition*, Washington, D.C.: American Psychological Association, 1991, pp. 3127-149.

13. Coakley, T. P., ed., *Issues of Command and Control*, National Defense University, Washington, 1991.

14. Darilek, R., et al, Measures of Effectiveness for the Information-Age Army, RAND MR-1155-1, 2000.

15. Dhillon, B. S., Mechanical Reliability: Theory, Models and Applications, AIAA Education Series, 1988.

16. Duda, R. O., and Hart, P. E., Pattern *Classification and Scene Analysis*, John Wiley, 1973.

17. Endsley, M.R., "Situation Awareness Global Assessment Techniques (SAGAT)," *Proceedings of the IEEE National Aerospace Conference*, Vol. 3, Hawthorne, CA, United States, May 23 – 27, 1988, pp. 789-795.

18. Friedell, M. F., "On the Structure of Shared Awareness," *Behavioral Science*, Vol. 14, No. 1, 1969, pp. 28-39.

19. Greenhalgh, C., Benford, S. and Reynard, G.,"A QoS Architecture for Collaborative Virtual Environments," *Proceedings of Seventh ACM International Conference on Multimedia*, Orlando, United States, October 30-November 5, 1999, pp. 121-130.

20. Hall, R. W., Mathur, A., Jahanian, F., Prakash, A. and Rassmussen, C., "Corona: A Communication Service for Scalable, Reliable Group Collaboration Systems," *Proceedings of the ACM 1996 Conference on Computer Supported Cooperative Work*, Boston, United States, November 16 – 20, 1996, pp. 140-149.

21. IEEE Standard Dictionary of Terms, 6ed., IEEE Publications, N.Y.

22. Jackson, B.W., and Thoro, D., *Applied Combinatorics with Problem Solving*, Addison Wesley, 1990.

23. Kraut, R. E., Miller, M. and Siegel, J., "Collaboration in Performance of Physical Tasks: Effects on Outcomes and Communication," *Proceedings of the ACM 1996 Conference on Computer Supported Cooperative Work*, Boston, United States, November 16 – 20, 1996, pp. 57-66.

24. Kreyzig, E., Introductory Functional Analysis, Wiley, 1978.

25. Lewis, D. K., "Scorekeeping in a Language Game," *Journal of Philosophical Logic*, Vol. 8, 1979, pp. 339-359.

26. Mandviwalla, M., and Olfman, L., "What do Groups Need? A Proposed Set of Generic Groupware Requirements," *ACM Transactions on Computer-Human Interaction*, Vol. 1, No. 3, 1994, pp. 245-268.

27. McDaniel, S. E., "Providing Awareness Information to Support Transitions in Remote Computer-Mediated Collaboration," *Conference Proceedings on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April 24-29, 1993, pp. 269-276.

28. Mitchie, et al in Aggarwal, J. K. ed. *Multisensor Fusion for Computer Vision*, Proceedings of the NATO Advanced Research Workshop on Multisensor Fusion for Computer Vision held in Grenoble France, June 26-30, 1989, Springer-Verlag, 1991.

29. Neter, J. and Wasserman, W., *Applied Linear Statistical Models*, R.D. Irwin, 1974.

30. Nichols, LTC Patrice, *U.S. 2025 Information Dominance*, Briefing, Army Communications-Electronics Command Research Development and Engineering Center Fort Monmouth, New Jersey, titled, June 1999.

31. Patel, U., D'Cruz, M. J., and Holtham, C., "Collaborative Design for Virtual Team Collaboration: a Case Study for Jostling on the Web," *Proceedings of the Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, Amsterdam, The Netherlands, August 18 – 20, 1997, pp. 289-300.

32. Pecht, M., (ed.) Product Reliability, Maintainability and Supportability Handbook, CRC Press, 1995.

33. Perry, W. "Knowledge and Combat Outcomes", *Military Operations Research Journal*, Vol. 4 No 1, 2000.

34. Perry, W., Moffat, J., "The Value of Information on the Outcome of Maritime Operations: The Use of Experts in Analysis", *Proceedings of 11th International Symposium on Operational Research*, Shrivenham, Wiltshire, UK, 5-9 September, 1994.

35. Perry, W. Moffat, J., "Measuring consensus in decision making: an application to maritime command and control", *Journal of the Operational Research Society (UK)*, (1997) 48, No. 4, pp. 383-390.

36. Perry, W. Moffat, J., "Developing Models of Decision Making", *Proceedings of 12th International Symposium on Operational Research*, Shrivenham, Wiltshire, UK, 5-8 September, 1995 and *Journal of the Operational Research Society*, (1997) 48 , No. 5, pp 457-470.

37. Perry, W. and Moffat, J., "Measuring the Effect of Knowledge in Military Campaigns", *Journal of the Operational Research Society,* (1997) 48, No. 10, pp 965-972.

38. Perry, W., Signori, D. and Boon, J., *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and its Impact on Shared Awareness,* RAND DRR 2389-OSD, 2001.

39. Perry, W. and Sullivan, T., *Modeling Information Processing With Recommendations for JWARS*, RAND DRR 1956-OSD/A, October 1999.

40. Perry, W. et al, *NATO and US Operations Relating to Kosovo, 1998-1999 (U),* RAND DRR-2243-A, 2000. This report is classified SECRET.

41. *Providing the Means*. U.S. Army Digitization Office. Washington, DC: Office of the Chief of Staff Army, 1994.

42. Pryor, J. B., and Ostrom, T. M., "Social Cognition Theory of Group Processes" in Mullen, Brian and George R. Goethals, ed., *Theories of Group Behavior*, New York: Springer-Verlag, 1987, pp. 147-183.

43. Russell, D. M., Stefik, M. J., Pirolli, P. and Card, S. K., “The Cost Structure of Sensemaking,” *Conference Proceedings on Human Factors in Computing Systems*, Vancouver, Canada, April 13-18, 1996, pp. 57-58.

44. Smith, D. R., *The Effect of Transactive Memory and Collective Efficacy on Aircrew Performance,* Dissertation, University of Washington, 1999, Ann Arbor, Mich.: University Microfilms, 1999, 05858900 388261.

45. Stalnaker, R. C., “Assertion” in Cole, P., ed., *Syntax and Semantics 9: Pragmatics,* New York: Academic Press, 1978, pp. 315-332.

46. Stark, H. and Woods, J. W., Probability, Random Processes and Estimation Theory for Engineers, Prentice-Hall, 1986.

47. The Penguin Dictionary of Psychology, © Arthur S. Reber 1995.

48. Ulhoi, J., and Gattiker, Urs E., “The Nature of Technological Paradigms: A Conceptual Framework”, Dorf, Richard, C., ed., *The Technology Management Handbook,* New York: CRC Press/IEEE Press, 1999.

49. “Understanding Information Warfare”, OSD Information Superiority Working Group, 2000.

50. Vin, H. M., Rangan, V. and Ramanathan, S., “Hierarchical Conferencing Architecture for Inter-Group Multimedia Collaboration,” *Conference Proceedings on Organizational Computing Systems*, Atlanta, United States, November 5-8, 1991, pp. 43-54.

51. Wagner, H., *Principles of Operations Research*, Prentice-Hall, 1969.

52. Waltz, E. and Llinas, J., *Multisensor Data Fusion*, Artech House, 1990.

53. Wegner, D. M., “Transactive Memory: A Contemporary Analysis of the Group Mind,” in Mullen, Brian and George R. Goethals, ed., *Theories of Group Behavior*, New York: Springer-Verlag, 1987, pp. 185-208.

54. Wellens, A. R., *Assessing Multi-Person and Person-Machine Distributed Decision Making Using and Extended Psychological Distancing Model*, Wright Patterson AFB, OH: Harry G. Armstrong Aerospace Medical Research Laboratory, Human Systems Division, Air Force Systems Command, AAMRL-TR-90-006, February 1990.