This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Information Sharing Among Military Headquarters

The Effects on Decisionmaking

Walter L. Perry

James Moffat

Prepared for the United Kingdom Ministry of Defense

RAND NATIONAL SECURITY RESEARCH DIVISION

A joint US/UK study team conducted the research described in this report. In the US, the research was carried out within RAND Europe and the International Security and Defense Policy Center of the RAND National Security Research Division, which conducts research for the US Department of Defense, allied foreign governments, the intelligence community, and foundations. In the UK, the Defence Science and Technology Laboratory (Dstl) directed the work and participated in the research effort. The RAND Corporation has been granted a licence from the Controller of Her Britannic Majesty's Stationery Office to publish the Crown Copyright material included in this report.

Library of Congress Cataloging-in-Publication Data

Perry, Walt L.
Information sharing among military headquarters : the effects on decisionmaking / Walter L. Perry, James Moffat.
p. cm.
"MG-226."
Includes bibliographical references.
ISBN 0-8330-3668-8 (pbk. : alk. paper)
1. Command and control systems—United States. 2. United States—Armed Forces—Communication systems. 3. Military art and science—United States—Decision making. 4. United States—Armed Forces—Headquarters. I. Moffat, James, 1948– II. Title.

UB212.P49 2004
355.3'3041—dc22

2004018584

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published 2004 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

New information technologies introduced into military operations provide the impetus to explore alternative operating procedures and command structures. New concepts such as network-centric operations and distributed and decentralised command and control have been suggested as technologically enabled replacements for platform-centric operations and for centralised command and control. As attractive as these innovations seem, it is important that military planners responsibly test these concepts before their adoption. To do this, models, simulations, exercises, and experiments are necessary to allow proper scientific analysis based on the development of both theory and experiment.

The primary objective of this work is to propose a theoretical method to assess the effects of information gathering and collaboration across an information network on a group of local decision-making elements (parts of, or a complete, headquarters). The effect is measured in terms of the reduction in uncertainty about the information elements deemed critical to the decisions to be taken.

Our approach brings together two sets of ideas, which have been developed thus far from two rather different perspectives. The first of these sets is the Rapid Planning Process, developed as part of a project on command and control in operational analysis models within the UK Ministry of Defence Corporate Research Programme. It is a construct for representation of the decisionmaking of military commanders working within stressful and fast-changing circumstances. The second set of ideas comes from the work on modelling the effects

of network-centric warfare, carried out recently by the RAND Corporation for the US Navy. We assess the effects of collaboration across alternative information network structures in prosecuting a time-critical task using a spreadsheet model. We quantify the benefits and costs of local collaboration using a relationship based on *information entropy* as a measure of local network knowledge. We also examine the effects of complexity and information overload caused by such collaboration.

Decisions in a Network

New technologies are enabling militaries to leverage information superiority by integrating improved command and control capabilities with weapon systems and forces through a network-centric information environment. The result is a significant improvement in awareness, shared awareness, and collaboration. These improvements in turn affect the quality of the decisionmaking process and the decision itself, which ultimately lead to actions that change the battlespace.

In this report, we focus on the quality of the decisions, or the planned outcome, rather than on whether or not the desired effect is eventually achieved.

We note that decisions are made based on the information available from three sources: information that is resident at the decision node; information from collection assets and information processing facilities elsewhere in the network; and information from other local decisionmakers with whom the decision nodes are connected and with whom they share information.

Rapid Planning Process

In most cases, decisionmakers must make decisions without full understanding of the values of the critical information elements needed to support the decisions. The decision taken depends on the current values of the critical information elements, which are dependent on the scenario. This dependency is modelled using the Rapid

Planning Process. The critical information elements map out the commander's conceptual space. In the basic formulation of the Rapid Planning Process, a dynamic linear model is used to represent the decisionmaker's understanding of the values of these factors over time. This understanding is then compared with one or more of the fixed patterns within the commander's conceptual space, leading to a decision.

A probabilistic information entropy model is used to represent the uncertainty associated with the critical information elements needed for the decision. Ideally, through the Rapid Planning Process, additional information from collection assets or from collaborating elements in the network serves to reduce uncertainty and therefore increase knowledge.

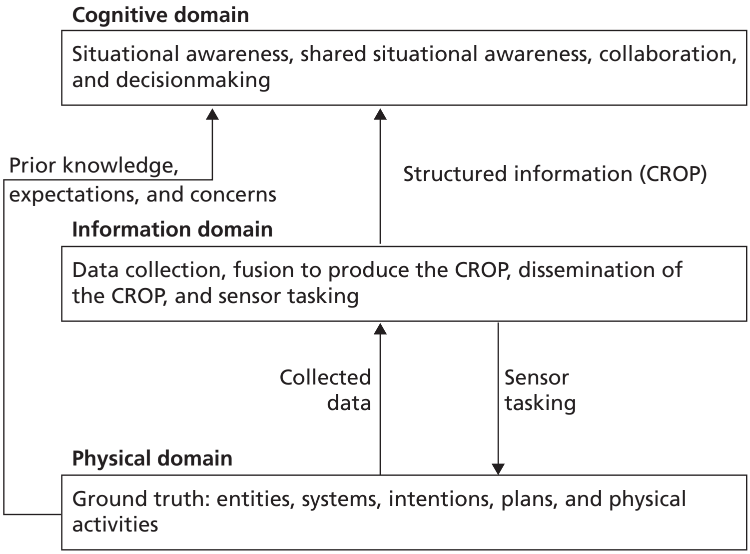
Knowledge

We are principally concerned with the information and cognitive domains, as depicted in Figure S.1. The domains of the information superiority reference model divide the command and control cycle into relatively distinct segments for ease of analysis. Their description includes the entities resident in the domain, the procedures performed and the products produced there, and the relationships among the domains.

Information derived from sensors or other information gathering resides in the information domain. This information is transformed into awareness and knowledge in the cognitive domain and forms the basis of decisionmaking. Our metrics quantify this process through the use of information entropy and knowledge measures.

Information sharing among nodes ideally tends to lower information entropy (and hence increase knowledge) partly because of the buildup of correlations among the critical information elements. That is, information can be gained about one critical information element (e.g., missile type) from another (e.g., missile speed). Such cross coupling is a key aspect for consideration, and we use conditional entropy to capture these relationships.

Figure S.1
The Information Superiority Reference Model



RAND *MG226-S.1*

Knowledge derived from entropy is a quantity that reflects the degree to which the local decisionmaker understands the values of the information elements. It is represented as a number between 0 and 1, with the former representing 'no understanding' and the latter representing 'perfect understanding'. From this knowledge, decisionmakers can assess whether or not they are in their 'comfort zone'—that is, whether the values of the key information elements support the decision they wish to take (such as one to launch the next attack mission).

Effects of Collaboration

Networks provide an opportunity for participating entities to share information as part of a collaborative process.[1] Here we focus on the synergistic effects of collaboration that improve the quantity (the completeness of our information) and the quality (its precision and accuracy) of the information needed to take decisions. We model the network as the combination of clusters of entities and represent each entity by a node. A cluster consisting of a single node is taken to be the degenerate case. Each such cluster consists of a set of entities, which have full shared awareness. *Full shared awareness* means that all entities in the cluster agree on the set of information elements and their values at any given time.

Estimators

Through observations of the battlespace, sensors and other information sources generate estimates for the information elements deemed critical to the decision. The uncertainty associated with the information elements is expressed in terms of probability distributions, the means of which are estimates of the ground-truth values. Because the mean of a probability distribution is a parameter of the distribution, we turn to parameter estimation theory to assess the quality of the information available to the decisionmaker and examine how the quality of the estimates contributes to knowledge.

- **Bias:** Bias in an estimate is error introduced by systematic distortions. An unbiased estimator is one for which its statistical expectation is the true value of the estimated parameter. That is, the expected value of the estimate of the parameter, $\hat{\mu}$, is the true value of the parameter, μ. The bias in the estimate is therefore the degree to which this is not true.
- **Precision:** The variation in estimates of the critical information elements can occur in a purely random way. Random errors

[1] *Collaboration* in this context is taken to be a process in which operational entities actively share information while working together towards a common goal.

affect the precision of the estimates reported because they increase the variance of the distribution of the estimated information element. In general, precision is defined to be the degree to which estimates of the critical information element or elements are close together.[2] Bias and precision, therefore, are independent—that is, biased estimates may or may not be precise.

Precision and Entropy

The amount of information available in a probability density is measured in terms of information entropy, denoted $H(x)$. Information entropy is always a function of the distribution variance, and therefore we use it as the basis for developing a knowledge function. For example, the bivariate normal distribution is $H(x,y)=\log|\mathbf{\Sigma}|$, where $\mathbf{\Sigma}$ is the covariance matrix. From this, we create a precision-based knowledge function as[3]

$$\begin{aligned} K(x,y) &= 1-e^{-\left[\log|\mathbf{\Sigma}|_{\max}-H(x,y)\right]} \\ &= 1-\frac{|\mathbf{\Sigma}|}{|\mathbf{\Sigma}|_{\max}} \end{aligned},$$

where $|\mathbf{\Sigma}|_{\max}$ is the determinant of the covariance matrix that produces the maximum uncertainty. Based on precision alone, $K(x,y)$ reflects the level of understanding within a cluster of decisionmakers.

For the simple case of two collaborating decisionmakers (i.e., two nodes of the network forming a cluster) who share two pieces of information with a multivariate normal distribution, the change in knowledge is given by

---

[2] This is a commonly accepted definition. Ayyub and McCuen (1997, p. 191) define precision as 'the ability of an estimator to provide repeated estimates that are very close together'. A similar definition can be found in Pecht (1995).

[3] Actually, the exact entropy value for the bivariate normal case is $H(x,y)=\log\left|(2\pi e)^2\Sigma\right|$. However, because we are concerned about the relative entropy, we use the simpler version, which we refer to as 'relative entropy'.

$$\Delta K = \frac{\rho_{1,2}^2 \sigma_1^2 \sigma_2^2}{\sigma_{1,\max}^2 \sigma_{2,\max}^2},$$

where $\rho_{1,2}$ is the correlation coefficient, σ_1^2, σ_2^2 are the variances, and $\sigma_{1,\max}^2, \sigma_{2,\max}^2$ are the maximum or bounding values on the variance for the two pieces of information.

Accuracy

Accuracy is the degree to which the estimates of the critical information elements are close to ground truth. The concept of accuracy comprises both precision and bias. In general, if a is an information element whose value x is unknown with probability distribution $f(x)$ and mean μ representing ground truth, then the bias associated with the estimate of the mean is $b = |\mathrm{E}(\hat{\mu}) - \mu|$, where $\hat{\mu}$ is the estimate of the mean. Because accuracy consists of both bias and precision, we therefore need a metric that combines both. One such metric is the mean square error (MSE), $\mathrm{E}[(\hat{\mu} - \mu)^2] = b^2 + \sigma^2$, where σ^2 is the variance of $\hat{\mu}$. The MSE is an extremely useful metric because it includes both accuracy in the total and precision as a component. In estimating ground truth, the bias accounts for nonrandom errors and the precision accounts for random errors.

We illustrate by continuing with the bivariate normal case. We assume that Bayesian updating is used to refine the location estimate based on the arriving reports. Bayesian updating is not always unbiased, and therefore we introduce systemic error. In this case, the bias is the Euclidean distance between the Bayesian estimate and the ground-truth value:

$$b = \sqrt{\left(\hat{\mu}_x - \mu_x\right)^2 + \left(\hat{\mu}_y - \mu_y\right)^2}.$$

By analogy with the MSE, the accuracy of the estimate is defined as $D(x, y) = b^2 + |\hat{\Sigma}|$.

The Effects of Bias, Precision, and Accuracy on Knowledge

We now account for bias, precision, and hence accuracy in the knowledge function by replacing the distribution variance with the MSE, or the accuracy measure $D(x,y)$ in the knowledge function. Therefore, for the multivariate normal case, we get a modified knowledge function of the form:[4]

$$K_M(\mathbf{x}) = 1 - \frac{b^2 + |\boldsymbol{\Sigma}|}{\left(b^2 + |\boldsymbol{\Sigma}|\right)_{\max}}.$$

The 'maximum mean square error' is a combination of the maximum bias and the maximum precision and represents the maximum in inaccuracy. Because bias and precision are independent, the maximum occurs when both are maximised, or $(b^2 + |\boldsymbol{\Sigma}|)_{\max} = b^2_{\max} + |\boldsymbol{\Sigma}|_{\max}$. Like the variance, a suitable upper bound for bias can be found by searching for the largest possible measurement error the sensors or sources might produce.

Completeness

In addition to precision and accuracy, collaboration also affects the completeness of the critical information elements available within a cluster. For the entire network, we assume there are a maximum of N critical information elements. For a given cluster, the total number required is $C \leq N$. However, at a given time, t, only $n \leq C$ might be available. If waiting for additional reports is not possible, a decisionmaker would be required to take a decision without benefit of complete information. Depending on his experience and other contextual information, the decisionmaker may be able to infer some likely less reliable value for the missing information. For now, we assume that if the value of an information element is missing, the value of completeness at cluster i is

[4] The subscript M denotes knowledge derived from the MSE.

$$X_{i,t}(n) = \left[\frac{n}{C}\right]^{\xi},$$

where ξ is a 'shaping' factor. For values of $\xi < 1$, the curve is concaved downwards; for $\xi > 1$, it is concaved upwards; and for $\xi = 1$, it is a straight line. The selection of the appropriate value depends on the consequences associated with being forced to take a decision with incomplete information as well as the commander's attitude to risk.

Information Freshness

A final consideration when assessing uncertainty is that of freshness. The information arriving at a decision node consists of reports concerning one or more of the critical information elements necessary to take a decision. Both precision and accuracy depend on the joint probability density function that reflects the uncertainty in our knowledge of the ground-truth fixed pattern at a decision node. These reports are used to update the joint probability distribution of the information elements and hence the probability of correctness of each of the fixed patterns in the local decisionmaker's conceptual space.

We have selected Bayesian updating as the method for combining reports from various sources and sensors. All things being equal, we desire to give more weight to more recent reports, which requires that we reevaluate all available, valid reports at the time a decision is to be taken. A time-lapse estimate, $0 \leq \Phi \leq 1$, is used to determine the rate of information decay so that old information is given less weight than current information.

Measuring the Overall Effect of Cluster Collaboration

Finally, we combine the currency-adjusted precision and accuracy knowledge function with completeness to arrive at a single metric to assess the effects of collaboration across the cluster. The ideal case is when we have full completeness, i.e., $X_t(n) = X_t(C) = 1$, and the knowledge shared across the cluster is fully accurate, $K_M(x) = 1$. Unfortunately, this ideal is seldom, if ever, achieved. Consequently, we require a construct that gauges the degree to which accuracy, as calculated here, and completeness contribute to knowledge.

In general, when $X_t(n)$ is small, the knowledge function should also be small. One way to reflect this behaviour is to replace the MSE in the entropy calculation with

$$\frac{b^2+\sigma^2}{X_t(n)}.$$

This equation has the desirable property that, when $X_t(n)\to 1.0$, the ratio is just the MSE, and when $X_t(n)\to 0$, it increases without bound. Because n is discrete, we can select $n=1$ to be the worse case, with $X_t(1)=C^{-\xi}$. Consequently, the upper bound on the resultant entropy calculation is

$$\frac{b_{\max}^2+\sigma_{\max}^2}{C^{-\xi}}=C^{\xi}\left(b_{\max}^2+\sigma_{\max}^2\right).$$

If $C=1$, there is no effect on the current entropy calculation or on the maximum entropy. If we let $K_\kappa(x)$ be the knowledge within the cluster based on accuracy and completeness, with the maximum variance replaced with $C^{\xi}(b_{\max}^2+\sigma_{\max}^2)$, we get

$$K_\kappa(x)=1-\frac{b^2+\sigma^2}{n^{\xi}\left(b_{\max}^2+\sigma_{\max}^2\right)}$$

for the univariate normal case.[5]

Up to this point, we have captured the effects of collaboration among decision nodes within a cluster on knowledge. The measured effects of information sharing through collaboration are accuracy and completeness. For the most part, these effects are dynamical, because they vary with the quality and quantity of reports received and processed over time. Missing from this analysis so far is an assessment of

---

[5] The κ subscript in this case refers to knowledge based on both the MSE and completeness.

the systemic effects of the network structure—that is, the effects that are more static. Next, we take up such measures of network complexity and combine them with the collaborative effects to arrive at a single measure of network performance and its effect on decision-making.

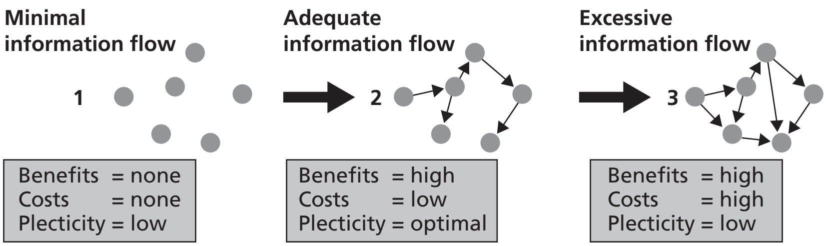
Effects of Structural Complexity

All networks exhibit complexity to a greater or lesser degree. Military command and control systems operating in a network-centric environment also exhibit complex behaviour. The challenge is understanding exactly what the complexity is, what its effects are, and how to quantify these effects. We note that there are both good and bad effects of complexity. Unfortunately, the term 'complexity' has a negative connotation; therefore, we have adopted Murray Gell-Mann's more neutral term, 'plecticity'.

In this context, *plecticity* refers to the ability of a connected set of actors to act synergistically via the connectivity between them. This measure is intended to take into account the fact that there may be constraints, due to technical or procedural limitations, on how nodes can constructively connect to other nodes; that is, a node's connectivity can add costs as well as benefits to the cluster. A measure of plecticity should account for the value of the cluster's ability to glean information from throughout the network to fulfil its particular functions, include a means for measuring the value of information redundancy, and reflect a cost to network effectiveness if nodes are overwhelmed.

For networks with inadequate clustering, as with excessive clustering—flows 1 and 3, respectively, in Figure S.2—we would expect low plecticity scores. The goal is to configure the information flow over a network with established link connectivity so as to maximise plecticity as measured in the terms discussed above and as illustrated by flow 2 in the figure.

Figure S.2
Overall Network Plecticity



RAND *MG226-S.2*

Accessing Information

The metric developed for completeness earlier is simply a ratio of counts: available required information elements to total required information elements. No attempt is made to assess the degree to which we can really *expect* to receive the information element, i.e., the degree to which the network allows the cluster to access information in the network. A metric that does so is the ratio of the aggregate expected degree of critical information access to the total number of required information elements. Such a metric accounts for the uncertainties associated with retrieving needed information.

We thus replace the binary accounting for information elements, with a connectivity score based on a distance function that recognises the cost imposed by the path the information must take through the network to arrive at the node requiring it.

For any information element, a_l, we are interested in the shortest path from source node to destination node, $d_l \geq 1$, however calculated. The restriction that the path distances always exceed 1.0 accounts for the fact that, for connectivity to exist at all, at least one link must exist between source and destination. The case in which no links exist implies an infinitely long path resulting in 0 connectivity. The quantity, d_l, represents the expense incurred by moving information element a_l from source to destination. The associated connectivity value is calculated as

$$k_l = \frac{1}{d_l^{\omega_l}},$$

where $\omega_l \geq 1$ is the rate at which k_l varies with changing values of the distance function.

The strength of the connectivity among all the nodes in such a path must take into account the vulnerability of path elements (links and nodes) to attack or failure. We can do this using the connectivity score described above by examining its value as we remove each node—link or both—one at a time from a given path. For simplicity, we consider only the loss of nodes. We create a depletion vector, $\mathbf{L}_l$, whose elements consist of the connectivity values for information element a_l, with each of the path nodes removed in turn. The vector $\mathbf{L}_l$ then represents the vulnerability of the path and, as such, expresses the degree of uncertainty associated with retrieving information element a_l from network sources. The adjusted connectivity for information element a_l from network sources to a single destination is calculated to be

$$k_l^* = k_l \left(1 - \frac{\|\mathbf{L}_l\|}{\mathbf{L}_l}\right)^{\frac{1}{\rho}},$$

where $|\mathbf{L}_l|$ is the cardinality of the vector $\mathbf{L}_l$ and ρ is the edge expansion parameter of the network, which measures the overall robustness and reliability of the network. The resulting formula for accessibility, $X(k)$, is

$$X(k) = \begin{cases} \left(\frac{k}{C}\right)^{\xi} & C \neq 0 \\ 1 & \text{otherwise} \end{cases},$$

where $k = \sum_{l=1}^{C} k_l^*$ and C is, as before, the total number of information elements critical to the cluster.

Benefits of Network Redundancy

Network redundancy focuses on the reliability of the network; its ability to deliver information in the face of node loss; system outages; inefficient operating procedures; or some combination of all these elements. At the same time, a network can deliver excessive information, thus causing delays because of the time and resources required to process all of it. Consequently, network redundancy can be both a cost and a benefit of the network information flow.

Needed information can be provided to a cluster from multiple sources. If the value of the information will change over time, we can expect multiple reports from each source. These multiple reports require combining in some way as previously discussed under collaboration. Whatever method is used, the degree to which the reports contribute to estimates close to ground truth and to a narrowing of the distribution variance, a benefit will accrue to the cluster because of redundancy. Recall that the total number of required information elements across the whole network is N; the number critical to a cluster is C, where $C \leq N$; and the number of these available within the cluster is n, where $n \leq C$. If we let the vector $\mathbf{\Theta} = [\Theta_1, \Theta_2, \cdots, \Theta_C]^T$ represent the aggregate value of reports received for each required information element $(a_1, a_2, \cdots, a_C)$ from $\mathbf{P} = [p_1, p_2, \cdots, p_C]^T$ sources, then we can construct a suitable normalised aggregate metric, $R(\mathbf{\Theta})$, as

$$R(\mathbf{\Theta}) = 1 - \frac{1}{n} \sum_{i=1}^{C} \gamma_i e^{-\delta_i(\Theta_i - 1)},$$

where $\gamma_i = 1$ if $p_i \geq 1$ and 0 otherwise. We let $r_i(\Theta_i)$ be the benefit accruing from obtaining reports on the value of information element a_i from p_i sources where $\Theta_i = \sum_{j=1}^{p_i} \theta_{i,j}$, and $\theta_{i,j} \in [1, \infty)$ measures the assessed reliability of the report on information element a_i from source s_j. The parameter, δ_i, reflects the relative importance of the information element, a_i.

The combined benefit of information redundancy information to the cluster, based on the conditional dependency between accessibility and redundancy, is

$$B\left[R(\Theta)\mid X(k)\right]=\frac{(\beta-1)\left[\kappa X(k)+\beta R(\Theta)\right]}{(\beta-\kappa)\left[\beta-X(k)\right]},$$

where $\beta>1$ is a constant that ensures a nonzero denominator and $\kappa\geq 0$ is another constant that ensures that the combined metric is bounded between 0 and 1.

Costs of Information Overload

At the same time, a network can deliver excessive information. The more sources of required information and the more frequent the reporting, the longer it takes for the cluster to get a coherent view of the situation. That is, it takes time to process information, which may or may not contribute to improving the quality of the estimates. This excess is referred to as 'information overload'. In addition, some of the sources may provide disconfirming evidence. The value of the disconfirming evidence can be good or bad, depending on the degree to which it reflects ground truth. Disconfirming evidence requires time to evaluate and therefore may increase uncertainty and decrease the quality of the estimates. Finally, it is also possible that raw data may be processed before being sent, thus arriving at the cluster as time-stamped information with the time at which the processing ended. This possibility introduces an artificial latency that contributes to uncertainty.

The supply of unneeded information to a cluster has an immediate negative impact, because it must be processed or, at a minimum, interferes with the receipt of needed information. However, as more unneeded information is supplied, its impact is reduced. Thus, a good function to model this behaviour is the exponential $U(m)=1-e^{-\nu m}$, where m is the number of sources of unneeded information and ν is a scaling parameter.

The costs of information overload associated with needed information within a cluster are generally minimal for low levels of redundancy. Indeed, at these levels, the benefits far outweigh the costs, as discussed earlier. However, at some point, costs rise sharply so that the marginal cost of an additional source of information is greater than the previous source. At some further point, this cost then levels off so that the marginal costs are minimal. This behaviour is best described using a logistics response function for each information element shared within the cluster. For simplicity, we express the combined costs of oversupply of needed information as a simple sum,

$$G(\mathbf{P}) = \frac{1}{n}\sum_{i=1}^{C}\delta_i \frac{e^{-(\chi_i+\varphi_i p_i)}}{1+e^{-(\chi_i+\varphi_i p_i)}},$$

where χ_i and φ_i are shaping parameters.

In considering the overall costs for the cluster, a balance is struck between costs of needed and unneeded information. We use a simple weighted linear sum of the two components of information overload, or $O[U(m),\mathrm{G}(\mathbf{P})] = \alpha U(m) + (1-\alpha)G(\mathbf{P})$, where $0 \le \alpha \le 1$, as a relative weight parameter.

Redundancy-Based Plecticity

The next step is to combine the costs and benefits of plecticity for a cluster associated with the mission at hand. For each cluster in the network, the measure of network plecticity, $C(B,O)$, is calculated as follows:

$$C(B,O) = B\left[R(\Theta)\middle|X(k)\right]\left[1 - O\left[U(m),G(\mathbf{P})\right]\right].$$

Network Performance

The last step is to combine the redundancy-based plecticity with the benefits of collaboration across all the clusters of the network. Our collaboration metric quantifies the effects of information sharing across a cluster on information completeness and accuracy, whereas plecticity measures the positive and negative effects of redundant information and the degree of information access. The former assesses the dynamic nature of the operation conducted on the network; the latter measures the effects of the underlying network structure and is therefore systemic. All the dependencies among the several components of collaboration and plecticity are not generally well understood. However, we know that high-quality performance requires good cluster knowledge and the means to share it and that scores in either category are penalised by deficiencies in the other. Therefore, the measure of total network performance is taken to be

$$\Omega\left(\Pi,\mathrm{K}_N\right)=\sum_{i=1}^{L}\left[C_i\left(B,O\right)K_{i,\kappa}\right]^{\omega_i},$$

where $\sum_{i=1}^{L}\omega_i=1$ and L is the number of clusters.

For values of $\Omega(\Pi,\mathrm{K}_N)$ close to 1.0, the network is performing well by producing the information required to take decisions within each of the clusters when required. However, this is not the whole story. The next step is to assess how well the combat mission is accomplished. As important as good decisions are, good combat outcomes are the ultimate measure of the value of network-centric operations. An example application shows how these approaches can be combined. The mathematical approach is used to filter out preferred network and clustering assumptions, which are then tested in a simulation environment. This allows the development of both network-based Measures of Command and Control Effectiveness and higher-level Measures of Force Effectiveness.