2006 CCRTS

THE STATE OF THE ART AND THE STATE OF THE PRACTICE

Title of Paper: Metrics For Assessing Command, Control, And Communications Capabilities

Topics: C2 modeling and simulation, C2 metrics, information operations/assurance, C2 experimentation

Name of Author(s): Martin R. Stytz and Sheila B. Banks
Point of Contact: Martin R. Stytz
Name of Organization: Institute for Defense Analyses
Complete Address: 1475 North Highview Lane, #104, Alexandria, VA 22311
Telephone / Fax: 407.497.4407; 703.338.2997
E-mail Address: mstytz@att.net, mstytz@ida.org

METRICS FOR ASSESSING COMMAND, CONTROL, AND COMMUNICATIONS CAPABILITIES

Martin R. Stytz, Ph.D.
Institute for Defense Analyses
Alexandria, VA
(407) 497-4407 (703) 338-2997
mstytz@ida.org , mstytz@att.net

Sheila B. Banks, Ph.D.
Calculated Insight
Orlando, FL
(407) 353-0566
sbanks@calculated-insight.com

ABSTRACT

The US military is undertaking an unprecedented transformation as a result of its adoption of a network centric operational philosophy. This transformation maximizes the military's reliance upon data superiority and decision superiority. However, we have yet to develop the metrics and insights necessary to fully exploit experimental and simulation capabilities needed to improve command and control and to assess command, control, and communications (C3) alternatives in a quantitative manner. The lack of C3 metrics also compounds the difficulties associated with developing the necessary doctrine, systems, and data insights to improve teamwork and team performance. The absence of relevant C3 metrics further confounds the ability to make measurable C3 improvements. Therefore, we undertook the development and study of metrics that can be used to assess C3 performance along a number of axes within any C3 architecture and in support of a variety of experiments. The metrics that we developed permit us to draw conclusions concerning key properties of each configuration and determine the configuration that best suits a given set of requirements.

Metrics are needed to gain insight into the performance of a C3 configuration. At its root, metrics must enable us to understand the data volume and data velocity capabilities that the configuration provides. Proper metrics allow us to measure the volume of data in transit at any time, the velocity of data movement from source to recipient, timeliness of data arrival, and the handling of priority data and, thereby, determine the overall efficiency of information handling within an organization's network centric infrastructure and to determine if the infrastructure and organizational policies promote network centric operations. These objectively determined metrics combined with additional derived metrics allow us to start to indirectly measure the overall situation awareness of the team or group as well as the ability of the team or group to operate efficiently and process multiple situations simultaneously and effectively. While these metrics do not paint a comprehensive picture of the performance of a C3 architecture, they provide the basis for insight. Our work built upon foundational research, as detailed in many sources such as the NATO Code for Best Practices for Command and Control Assessment, to assemble a set of metrics that can be used to provide new insights into the effectiveness of various C3 configurations. In this paper, we discuss the development of the metrics, their basis, and their use.

1. Introduction

The US military is undertaking an unprecedented transformation as a result of its adoption of a network centric operational philosophy [1-7, 9, 10]. Historically, whenever a dramatic or disruptive change in military technology takes place, there is a period of uncertainty when it is unclear how to properly use the technology and resources are wasted in misguided operational deployments. Nations that achieve an early understanding about the proper employment of the disruptive technology can gain a strategic and/or tactical advantage. The dramatic increases in computational and networking technologies that enable network centric technology ushers in a new suite of disruptive technologies, along with the concomitant uncertainties concerning employment and doctrine for the technologies. While many of the effects of the network centric transformation are unclear so far, some aspects of the effect of the transformation are now obvious and some technology needs that the network centric transformation will impose are also coming to light. In this paper, we address one of the technology needs that have arisen, the need for metrics to assess the efficacy of the employment of the technologies as well as the utility of policy and doctrine governing the use of the technology.

One obvious effect of the network centric warfare transformation is to greatly increase the military's reliance upon data superiority and decision superiority to achieve overwhelming battlespace dominance. Because of this transformation, computer networks and the data they carry are now, more than ever before, viewed as force multipliers and critical assets that are essential to military operations. As a result of the increase in the importance of military computer networks and their data, there has been a corresponding increasing emphasis on addressing the implications of adopting a network centric operations orientation with regard to policy, military doctrine, computational power, and aggregate bandwidth / communications requirements. As a result of this research and corresponding commercial technological developments, there has been a parallel increase in network bandwidth and computational power available for operational needs. Policy and doctrine have also been expanded upon and developed to illuminate techniques for best employing the increased network and computational power to achieve decision superiority. And yet, it is clear that the improvements in bandwidth, computational power, policy, doctrine and tactics do not result in a commensurate, corresponding increase in operational effectiveness because of uncertainty about the proper approaches to employ to conduct effective network centric operations. In short, our investments in improved data transport and computational capabilities and in our understanding of the network centric environment have not been as effective as would be reasonably expected.

One reason, possibly among many, for this relative ineffectiveness is that we do not have an objective analytical capability for assessing alternatives and tradeoffs in technology capabilities. Another reason is that we do not have a capability to assess the effects of different technology, policy, and doctrine choices upon network centric operations and warfare. While we know how to knit together advances in physical capabilities (bandwidth and computational power) to increase, in an absolute sense, the available bandwidth and computational power, we lack a framework that can tie these advances to network centric policies and doctrine that maximize the effectiveness of available technological resources. Recall that the goal of developing the network centric warfare philosophy is to achieve a dynamic, flexible, dominant network centric force. Nevertheless, we lack the analytical tools needed to successfully chose from among the many technology, policy, and doctrine options that are available in order to make choices that best employ available resources in conjunction with effective doctrine and policy. Our work was undertaken to address this shortfall by developing an analytical foundation that will allow us to understand the effects of technology deployment and policy and doctrine changes.

Simulation is one tool that can be used to indicate how best to knit together technology, policy, and doctrine to yield an effective network centric operational force. Within a distributed interactive simulation environment that models network centric operations, all of the differences that influence joint military operations, such as armed forces structures, doctrine and missions, must be accurately portrayed in a simulation environment. At the same time, the distributed interactive environment must also readily support experimentation in all aspects of network centric coalition military operations, including procedures, techniques, doctrine, and tactics. A network centric operations simulation environment must also aid in the development and evaluation of new coalition procedures, techniques, doctrine, and tactics. But, providing a network centric distributed interactive simulation environment that creatively and accurately emulates operations is expensive and time consuming. Simulation, alone, cannot be used to evaluate all the options available to us for network centric operations. An underlying analytical framework is needed that can be used to evaluate candidate approaches and identify those which are most promising. The most promising approaches can then be evaluated further within a simulation environment, using the same analytical tools but with more detailed data. Our research objective is to develop this analytical framework.

The paper is organized as follows. Section Two holds a brief discussion of the motivation for our research effort. Section Three contains a discussion of previous research related to our work. Section Four presents the development of the analytical framework and metrics that we propose. Section Five contains a discussion of the insights that the framework and metrics can provide in the quest to knit technology, doctrine, and policy into a cohesive, responsive, effective network centric force. Section Six contains a discussion of the policy implications that the framework and metrics suggest. Section Seven contains a summary of our research to date and suggestions for further research in this field.

2. Motivation

A network centric force is effectively networked by its network capacity and data infrastructure. A network centric force has the capability to share and exchange data among the distributed elements of the force and has access to data whenever and wherever it is needed. However, current policies for data sharing and network operations can inhibit achievement of this goal, and without metrics we are unable to determine when or if this has happened.

The motivation for our research is to redress the lack of a capability for analysis of command and control structures, policies, doctrine, and technologies. In addition to the analytical shortfall, we want to address the derivative problem of translating human formulated policies into machine-actionable policies that maximize the use of network and computational resources for network centric operations. Therefore, we must learn how to express doctrine and strategy as network and computational management policies that can be evaluated. This requirement calls for an expression of a relationship between the two aspects: doctrine/policy and technology. To achieve this goal, we must learn how to express intellectual decisions concerning policy as network bandwidth allocations and other network/computational policies. Therefore, control and management of network resources[1] and the data that move across them are two crucial topics that must be addressed in developing an analytical capability if we are to gain maximum operational advantage from investments made to develop network centric operational capabilities. Unfortunately, these two topics as well as the technological issues related to automatically translating command-level policy into network and data management policy are topics that, to date, have received little research attention to date. Our goal is to examine these issues and provide insight into the decision space that must be mastered and from this vantage develop foundational analytical tools.

The analytical foundation is critical because it can guide the employment of network and data control and management policy, which are of critical importance to the success of network centric operations. These items are important for two reasons. First, these two classes of policies address implementation of network centric operational needs. Second, these policies are the only mechanisms available to commanders for insuring that the right data reaches the right user at the right time. Since network centric operations rely upon data and decision superiority coupled with rapid resource re-allocation to achieve decisive battlespace dominance, the network and data control and management policies must be established across the network in light of the needs and capabilities of the individuals who rely upon the network and its data. The analytical framework would help in the determination of the necessary policies. By having the proper analytical foundation in hand, the network and data policies that are employed can support user needs and requirements while also considering individual data needs for decision-making, the available bandwidth, the communication alternatives, the various mission priorities, and individual data security needs. The network and data policies can satisfy the users' requirements in a number of ways; by allocating bandwidth to users, by allocating bandwidth for policy propagation, by allocating bandwidth for the transmission of assessments of user data needs, and by allocating different priorities to the different types of data as it moves between users. Because changes in network and data control and management policy must be made rapidly, tools that accurately translate the command-level policy decisions into network and data control and management policies are needed, which further argues for an analytical framework for analysis that can be automated.

Clearly, the network and data policy requirements are driven by five factors: 1) the mission for each organization on the network, 2) the current state of the battlespace, 3) the available communication channels within the organization, 4) the data needs for each user and commander, and 5) security requirements for each user and commander. These factors combine to define the data volume and latency needs for each user, thereby specifying the instantaneous bandwidth requirements for each user and the network security requirements, which must be accounted for in the analytical framework. The five factors also define the instantaneous data veracity/truthfulness and data verification requirements for each user. Network and data policy choices are complicated by the fact that data needs will be different for each user and unit. Circumstances often alter user and unit needs for data and thereby force the development of dynamic policies and dynamic policy change. Therefore, data and network policy as it relates to each user and each unit, must change rapidly in order to effectively address their needs. The dynamic nature of data and network policy further complicats the analytical framework. The variety of demands placed upon network and data services coupled with the need for rapid change in network and data policies point to the need for intelligent agent assistance and human behavior models for each user to aid in network and data policy development. These technologies will aid in rapidly allocating resources in accordance with the guidance provided by the framework. Intelligent agent assistance and human behavior models are essential to the process of rapidly translating command-level policy decisions into network and data control and management policies. The need for intelligent assistants and human behavior models has been suggested as a response to the complexity and variety of the data available to each user in a network centric environment. The need for intelligent assistants and human behavior models is increased by the necessity for rapidly adapting network and data policies to changes in the five factors to effectively manage the network environment. An analytical framework can be used by intelligent assistants to guide their decision making. Our research is intended to develop an analytical framework that can be

---

[1] The difficulties encountered in control and management of resources is a topic receiving more attention of late; see, for example, "An AI Planning-based Tool for Scheduling Satellite Nominal Operations," by Moreno, Borrajo, and Meziat, *AI Magazine*, vol. 25, no. 4, Winter 2004, pp. 9-27.

used for a number of purposes. The uses include the ability to address the factors highlighted above and to uncover the requirements for network and data policy, to explore the effects of decision-making data demands on network and data policies, and to examine the effect of network and data policy on the efficiency of network-enabled operations. The analytic framework can also help to uncover the requirements for the tools needed to knit together current and coming network centric operational capabilities into an effective network centric operational force.

To address the many issues raised above there is a pressing need for an improved abstract understanding of data transport and network capabilities. We must also be able to understand the interplay between them, doctrine, and policy. There is a further need for metrics that allow us to measure progress in addressing these issues. We found little prior work that we could draw upon to either improve our understanding or that would provide network centric relevant metrics. In this paper, as part of the analytic framework, we develop a suite of metrics that addresses the need for network centric relevant metrics and that allows us to determine the effect of changes in policy and doctrine in a network centric relevant manner.

3. Network Centric Warfare Background

To prepare for military operations, it is necessary to "Train the way you will fight," which has been the policy for United States' military training. This philosophy has served the warfighter well as evidenced by the many successful operations executed around the world over the last decade. However, the US military is in the midst of a change in its philosophy, approach, and technologies used for warfare. These changes move us toward small formations, small but extremely accurate weapons, and high speed movement all augmented by rapid, automated movement of data between and among all military components from the battlefield back to the logistics depot. This new form of warfare, in which a great premium is placed upon timely, accurate data, is called network centric warfare (NCW) [1-7, 9, 10].

In the network centric approach to warfare, information technologies are exploited to the maximum extent in order to increase the effectiveness and efficiency of all military operations. To leverage information technologies to the desired degree requires that information move from sensors to operators as well as between all humans involved in all aspects of military operations with unprecedented speed, accuracy, and security so that the information is both trustworthy and arrives wherever it is needed when it is needed. Simply achieving the required velocity, veracity, and security for information within a national joint operations network in order to attain a network centric operational capability poses a number of technical challenges. The challenges include providing sufficient bandwidth to meet the additional communication burden, securing information, and routing the information in a timely manner between information producers and consumers. For this future vision of warfare to be achieved and be effective there are a number of issues that must be addressed and solved in the real-world and in the world of simulation. In the NCW battlespace of the future, the coming capabilities in networks and computing portend a time when warfighters will become very dependent upon the unprecedented level of detailed data available concerning the situation within a battlespace. This reliance will induce foes to attempt to disrupt the data flows in an attempt to gain an advantage or to disrupt friendly operations. The interplay between friendly efforts to maintain their data operations and enemy attempts to disrupt them will inevitably result in conflict in the cyberworld, or cyberbattlespace.

Network centric operations are military activities that are enabled and enhanced in effectiveness by the networking of the force. The ability to operate in a network centric manner provides warfighters with a new type of data advantage, an advantage broadly characterized by significantly improved capabilities for sharing and accessing data. Network centric warfare enables networked warfighters to leverage their data advantage to increase their effectiveness across a broad spectrum of mission areas. The key to this increase in effectiveness is data superiority. Data superiority is a state in the data domain wherein one adversary is able to establish a superior data position as regards other adversaries. Data superiority is enabled by an imbalance in the data domain but this imbalance can only be fully exploited by a network centric force.

Our general thesis and the motivation for our research is that as the network centric warfare model for warfare is embraced as the paradigm for military operations, the network and associated software will become increasingly important and lucrative targets for an adversary. In light of this thesis, operators and information technology specialists must be able to recognize and counteract either an attack or an attempt to conduct an exploit against information resources. Operational units and information technology specialists must also be able to differentiate between an attempted exploit/attack[7-15] and a system failure or fault. So, as we improve our efficiency and effectiveness through the use of networking and computational resources, we also increase our reliance upon computers and communications systems in a network centric cyber battlespace. Because of this reliance upon a set of resources, attacks are inevitable and information technology specialists, commanders, and other users must be

able to determine if an attack is underway, diagnose the attack, and take appropriate corrective action within the cyber battlespace. The key to preparation for this new battlespace is development of new distributed simulation training systems that allow trainees to learn about the practical application of the metrics that measure the performance of the network centric environment.

Network centric warfare simulation is especially difficult. A few examples will illustrate the difficulty. Webster and Gallant[11] discuss the challenges inherent in connecting arbitrary battlefield functional areas and their impact upon operational architectures and force effectiveness. Alexander[12] discusses the challenges inherent when integrating legacy simulations to portray a network centric operational environment, especially the challenges posed to Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) integration and portrayal.

Mathis[13] examines the problems inherent in portraying Future Combat Systems (FCS) set of capabilities within a network centric operational environment in order to better understand the tradeoffs to be made when crafting a FCS force in a Joint Virtual Battlespace (JVB). Snively, et.al.[14] address the issues faced when designing a large-scale HLA compliant federation to portray a JVB and how these issues force changes to the HLA Run-Time Infrastructure (RTI). These five papers point out and discuss the challenges posed when linking together disparate simulations that portray entity and aggregate level simulation environments and of representing information flows in a network centric environment, but their emphasis is on US military needs. Turrell et.al.[15] discuss the challenges posed to NATO simulation environments and the tool repository that has been developed to improve the efficiency of simulation environment development for NATO purposes. Tolk[16,17] discusses various NATO M&S efforts, the need to coordinate and integrate these efforts and make them interoperable, and of the need to merge and coordinate these disparate efforts across NATO in order for them to be advantageous to all of NATO. Falzon, et.al.[18] discuss an Australian effort to use modeling and simulation to support operational planning, but is an aggregate simulation and so does not address in detail the challenges posed by the need to model the variations in individual behavior that will be important in a network centric operational environment.

The challenge posed by the network centric paradigm for warfare is not confined to the simulation arena. Network centric warfare is especially demanding as it spans the entire spectrum of conflict. However, a number of issues arise that must be addressed in order to assure accurate information operations within a network centric warfare environment. When performing military planning and operations in a network centric warfare environment, the operation and use of computer networks and software will increase in importance. This increasing reliance points to a need for training of operators that use the network so that they can gain the maximum advantage from the available information and also be able to recognize when the information is incorrect and/or the network and software are not functioning properly. However, in spite of the clear need for the development of operators with broad and deep expertise in defending against information attacks, we currently have no capability to address the need to train operators to recognize and counter cyber attacks upon network resources. Development of expertise, let alone the deep and broad capability for conducting rapid, effective defensive actions, is currently beyond the ability of any currently available training system, but must be developed. The metrics and formulations presented in this paper will assist in assembling these environments and evaluating the choices made by people who use them.

4. Development of the Analytical Framework

Clearly, the ability of a network centric force to operate effectively is correlated with the ability of data to move through the organization effectively and efficiently. However, the obvious accuracy of this statement does not provide sufficient guidance to effectively assess the quality of the data flow, to develop and assess doctrine and policy, and to identify areas within the organization where changes in policy and data flow processes can be changed to the greatest positive effect. To help provide the necessary guidance, we require a formal statement of the objectives for data movement within an organization.

Within a network centric organization, there are two sets of entities, sources of data and recipients of data. Within the organization, let *r* be the set of data recipient entities and allow them to be arbitrarily and uniquely labeled from 1 to n. Within the same organization, let *s* be the set of data source entities and allow them to be arbitrarily and uniquely labeled from 1 to m. Let I_r be the data required by/destined for a particular recipient of data and *n* be the number of data recipients and let I_s be the data sent from any source of data and *m* be the number of data sources. Then, $I_r \leftarrow I_s$ defines the instantaneous data volume (in bytes) between all sources, s, and recipients, r, of data. We can then define $\mathbf{I_1}$ as:

$$\mathbf{I_1} = \left(\prod_{i=1}^{n} I_{ri} \leftarrow \prod_{j=1}^{m} I_{sj} \right) \qquad \textbf{(1)}$$

Therefore, $\mathbf{I_{1_1}}$ is the total instantaneous volume of data moving from all sources of data to all recipients of data within an organization at any given time. Note that this definition is source-recipient topology neutral, technology neutral, and bandwidth independent. This definition also accounts for data moving on the network for both operational and network management purposes. Based this definition for $\mathbf{I_1}$, it is clear that for a network centric force to be effective, its data capacity must not only be able to accommodate peak demands for transmission of operational data but also peak demands for transmission of operational data in conjunction with simultaneous peak demand for transmission of network management data. Clearly, $\mathbf{I_1}$ is always less than or equal to the maximum data volume demand imposed by an organization during an operation. In addition, the data transmission capacity for an organization must be equal to or greater than $\mathbf{I_1}$ if an organization is to be network centric. Using $\mathbf{I_1}$, we define the instantaneous data velocity $\boldsymbol{\varpi}$ within an organization at a given time $\boldsymbol{\tau}$ within an organization as follows in equation 2. The mean data velocity $\boldsymbol{\varpi_m}$ for an organization over a given time interval $\boldsymbol{\gamma}$ can then be defined as shown in Equation 3.

$$\varpi_\tau = (I_{1_\tau} - I_{1_{\tau-1}}) / I_{1_{\tau-1}} \tag{2}$$

$$\varpi_m = \left(\sum_{\tau=1}^{\gamma} \varpi_\tau \right) / \gamma \tag{3}$$

A network centric organization should strive to attain a high value for $\boldsymbol{\varpi_m}$ as well as a high value for $\boldsymbol{\varpi}$ during important periods of activity. However, as important as this value may be for an organization, other types of information flows are also of crucial importance to a network centric organization. Two of these types of information flows are the ability of the organization's infrastructure to give expedited handling to important (or priority) information and the ability of an organization's infrastructure to provide communication connectivity between high priority communicants. To determine if the organization's infrastructure appropriately addresses these two types of information handling, we must first determine how well, on average, the organization's infrastructure supports information flows between all senders and recipients of information. Let the expression ($r_i \leftarrow s_i \neq 0$) be used to indicate that there is message traffic between a given recipient and transmitter of information. Let $\mathbf{I_{2_\tau}}$ be the average time required for data to move from all sources to all recipients within an organization for a given time period $\boldsymbol{\tau}$, then $\mathbf{I_{2_\tau}}$ can be defined as in equation 4. $\mathbf{I_2}$ for a given time interval, $\boldsymbol{\gamma}$, is calculated as shown in Equation 5.

$$I_{2_\tau} = \left(\left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j} \right) \right) \div \sum_{i=1,j=1}^{n,m} \left(\Delta t \left(r_i \leftarrow s_j \right) \ \ \forall \ \left(\left(r_i \leftarrow s_j \right) \neq 0 \right) \right) \tag{4}$$

$$I_2 = \left(\sum_{\tau=1}^{\gamma} I_{2_\tau} \right) / \gamma \tag{5}$$

Clearly, for a network centric organization to be effective, $\mathbf{I_{2_\tau}}$ must be as large as possible for all time periods and $\mathbf{I_2}$ must also be maximized over all time intervals. To insure that $\mathbf{I_{2_\tau}}$ and $\mathbf{I_2}$ are maximized, there must be little or no contention for bandwidth within the organization and operational and network management data must be transmitted with equal promptness. In addition, organizational data management policies must be formulated so that data is routed efficiently, even in case of failures of portions of the infrastructure, and so that information still reaches its intended destination in a timely manner even when the infrastructure is under physical or cyber attack. While efficient transmission of data is crucial to network centric warfare, not all data is of equal importance, as we have indicated above. So, even though $\mathbf{I_2}$ may be acceptable the organization may not be operating effectively from a network centric warfare perspective because higher priority information is not given corresponding higher precedence for transmission through the organization's infrastructure. Therefore, we not only require a metric in order to assess overall data transmission efficiency but also to assess how well the organization manages the transmission of priority data. The overall efficiency of data transmission for priority information is indicated by the

value of $\mathbf{I_3}$. Let $\mathbf{I_{3_p}}$ be the average time for priority data to move from all sources to all recipients of data of that given priority within any given time period $\boldsymbol{\tau}$ within an organization. Assume that data has only one priority or that it is handled in accordance with the highest priority level assigned to it. Assume there are *x* sets of priority data within that same time period, and let **p** represent a given data priority for data within an organization, clearly p can assume any value in the range 1 to x. Then $\mathbf{I_{3_p}}$ for a given message priority *p* at a time $\boldsymbol{\tau}$ is defined as shown in equation 6. With this specification in hand, we define $\mathbf{I_3}$ for all message priorities within an organization at a given time $\boldsymbol{\tau}$ as shown in equation 7.

$$\mathbf{I_{3_p}} = \left(\left(\prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j}\right)\right) \Big/ \sum\left(\Delta t\left(r_i \leftarrow s_j\right)\left[\ni\left(\left(r_i \leftarrow s_j\right) \neq 0 \ \wedge \ \left(r_i \leftarrow s_j\right) \subset p\right)\right]\right) \quad \textbf{(6)}$$

$$\mathbf{I_3} = \sum_{p=1}^{x} \mathrm{I}_{3_p} \ / \ \mathrm{x} \quad \textbf{(7)}$$

$$\mathbf{I_{4_r}} = \sum_{j=1}^{m}\left(t_{a_r} - t_{n_r}\right) \ \forall \ \left(I_r \leftarrow \prod_{j=1}^{m} I_{s_j} \ \ni \ \left(r_r \leftarrow s_j\right) \neq 0\right) \quad \textbf{(8)}$$

Let $\mathbf{I_{4_r}}$ be the time differential between the time, t_n , when data (of all priorities) is needed by a recipient and the time, t_a , when it received by the recipient in a given time period. Then $\mathbf{I_{4_r}}$ for a given recipient ***r*** during that time period is defined as shown in equation 8. $\mathbf{I_4}$ for an organization within that same time period is defined as shown in equation 9.

$$\mathbf{I_4} = \left(\sum_{r=1}^{n} \mathrm{I}_{4_r}\right) / n \quad \textbf{(9)}$$

Clearly, $\mathbf{I_4}$ for an organization should be minimized in order to increase network centric effectiveness. In addition, it is clear that for a given recipient to receive the data of most importance to the recipient, $\mathbf{I_3}$ for the highest priority data for the recipient must be minimized in order to minimize $\mathbf{I_4}$ for the recipient.

We define $\mathbf{I_{5_r}}$ as the time differential between the time, t_n, when data is needed by a recipient and the time, t_r, when it received by a data recipient for a given time period for data of a given priority ***y***. $\mathbf{I_{5_r}}$ within a given time period is defined as shown in equation 10.

$$\mathbf{I_{5_r}} = \sum_{j=1}^{m}\left(t_{a_{r_j}} - t_{n_{r_j}}\right) \forall \ I_r \leftarrow \prod_{j=1}^{m} I_{s_j} \ \ni \left(\left(\left(r_r \leftarrow s_j\right) \neq 0\right) \wedge \left(\left(r_i \leftarrow s_j\right) \subset p\right)\right) \quad \textbf{(10)}$$

$\mathbf{I_{5_r}}$ needs to approach zero for data of the highest importance for each recipient during any time period in order for an organization to increase its network centric efficiency. Clearly, lower values for $\mathbf{I_5}$ are preferable, but the doctrine and policies for data movement within an organization should insure that $\mathbf{I_5}$ for data of higher priority are given higher priority within the network as well as by the sources and recipients of the data. Therefore, policies should be established such that priority data has a better chance of reaching a recipient when it is needed, which in turn forces $\mathbf{I_{5_r}}$ toward zero.

A final required metric is a measure that indicates how well an organization's infrastructure transports information between important senders and recipients of information. This measure would indicate how well important communicants, such as commanders, can exchange information. While an individual communication may not be critical, the fact of the communication may be important and the need for ongoing communication between important communicants may also be important. We use $\mathbf{I_6}$ to represent the efficacy of communication between

important communicants at a given time period. Let members of the important transmitters of information be members of the set $\mathcal{T}$ and be designated by $\underline{t}$, and let members of the important recipients of information be represented by $\mathcal{R}$, and let the members of the set be designated by $\underline{r}$. Let $\mathbf{I}_{6_{\underline{t},\underline{r}}}$ represent all communications between a priority transmitter and a priority recipient. We can then examine the time differential between the time that information is needed by a priority recipient from a priority transmitter and the time that it arrives from the same transmitter. As with our other measures of network centric performance, this variable, too, should be minimized for each transmitter and receiver pair. If we let Π represent the total number of priority sender and receiver pairs in an organization and let **p** represent a single priority sender and receiver pair, then $\mathbf{I_6}$ for an organization at a given time period is represented as shown in Equation 12.

$$\mathbf{I}_{6_{\underline{t},\underline{r}}} = \sum_{j=1}^{m}\left({}^{t}a_{r_j} - {}^{t}n_{r_j}\right) \forall \left(\left(\mathop{\Gamma}_{i=1}^{n} I_{r_i} \leftarrow \mathop{\Gamma}_{j=1}^{m} I_{s_j}\right) \ni \left(\left(r_r \leftarrow s_j\right) \neq 0\right) \wedge \left(\left(r_i \in R\right) \wedge \left(s_j \in T\right)\right)\right) \tag{11}$$

$$\mathbf{I_6} = \left(\sum_{p=1}^{\Pi} \mathrm{I}_{6_p}\right) \Big/ \Pi \tag{12}$$

Of course, the crucial objective for the organization is to minimize $\mathbf{I_6}$ for the most important communicants and not for the entire organization. By examining the values for $\mathbf{I_4}$ and $\mathbf{I_6}$ for the same communicants for the same time periods, we can then determine if the organization's infrastructure gives proper priority handling to communication between important communicants.

5. Improving Network centric Information Transport

With these definitions in hand, we can return to $\mathbf{l_2}$ and examine it in more detail. For $\mathbf{l_2}$, the differential for a given recipient **r** is composed of the sum of the time the data is spent in a transmission medium, **m**, the time spent in computing devices, **c**, the time spent in sensing systems, **s**, the time spent in releasability decision making, **rdm**, and the time spent in human analysis, **h**.

$$\mathbf{l}_{2_{r_t}} = (\mathbf{t}_{r_m} + \mathbf{t}_{r_c} + \mathbf{t}_{r_s} + \mathbf{t}_{r_{rdm}} + \mathbf{t}_{r_h}) \tag{13}$$

Clearly, $\mathbf{t}_{r_m}$, $\mathbf{t}_{r_c}$, **and** $\mathbf{t}_{r_s}$ are approximately constant for any given operation and over relatively long periods of time and change slowly in relation to a given operation or in relation to the rate at which new technologies can be widely deployed. Therefore, the value for $\mathbf{l}_{2_{r_t}}$ is dominated by the values for $\mathbf{t}_{r_h}$ and $\mathbf{t}_{r_{rdm}}$. This result implies that network centric organizational policies should be established with the objective of minimizing the amount of time that data spends undergoing human analysis and the amount of time that data spends in the releasibility decision process. In fact, automation of these two processes would be an effective means to minimizing $\mathbf{I_2}$ in the short term since the values for the other components of $\mathbf{I_2}$ are dependent upon the overall progress of commercial networking technology, which by and large is influenced very little by government needs. This same conclusion appears to hold for $\mathbf{l_3}$, $\mathbf{l_4}$, and $\mathbf{l_5}$ as well. This conclusion agrees with our intuition because reductions in the time spent in human decision-making concerning releasilibility of data will improve the performance of the system when transporting important data to a recipient that needs the data. However, we have yet to scientifically demonstrate whether improving the performance of the system in one of its components in regard to these two parameters will insure an overall improvement in performance. Additional research in the system engineering and composition aspects of data transport mechanisms in regard to network centric warfare is required.

Another approach to improving system performance that has been suggested is the use of intelligent agents. If intelligent agents are to be used to improve the data flow within an organization, the first priority for their use is for making decisions for releasibility. Using intelligent agents for making this releasibility decision would apparently yield the biggest dividend for improved performance of the network centric organization, for data

movement within the organization, and to achieve the ultimate goal of improving timely decision making. Of course, improvements in decision-making will not occur if the user is overwhelmed with information[8], so the intelligent agents not only have to insure that the prioritized information reaches the user but also that the user is not inundated with information. Before moving on to a discussion of the policies suggested by the work presented in this section, Table 1 summarizes the major metrics/variables defined in this section and a short specification for each.

Table 1: Major Metrics/Variables and Their Definitions

Metric/Variable	Definition
I_1	The volume of data moving from all sources of data to all recipients of data within an organization at any given time
I_2	The average time for data to move from all sources to all recipients within a time period
I_3	The average elapsed time for priority data of a given priority to move from all sources to all recipients of data of that priority at any given time.
I_4	The time differential between the time when data is needed by a recipient and when it is received.
I_5	The time differential between the time when data is needed by a recipient and when it received by the data recipient for a given time period for data of a given priority.
ϖ_τ	Data velocity within an organization at a time τ
I_6	The efficiency of the movement of data between important communicants within an organization.

6. Policies and Tools

In the preceding section, we defined measures for data movement within an organization; measures that allow us to assess the efficiency of data flow, its velocity, the total data flow at any time, and measures to assess the ability of a data transport system to respond to the demands placed upon it during the course of an operation. In addition, we defined the metrics so that the data required to compute the figures of merit can be gathered. Nevertheless, while we have defined these metrics so that they can be applied to any combination of network configurations, it should be clear that we currently do not have the tools available to readily gather the required data, that we lack a scientific demonstration of the metrics, and we lack the engineering tools required to design networks with the capabilities required to optimize the measures. Nevertheless, from a theoretical point of view, we do have some insights into the general qualities that the data transportation system should possess. The system should be able to deal with rapid changes in data transportation requirements and allow data to reach its recipients rapidly. Also, data and network policies should be constructed so that prioritized data receives preferential handling and so that the data spends little or no time in the $\mathbf{t_{r_{rdm}}}$ state.

One clearly important parameter within a network centric organization is $\mathbf{I_1}$. The data transportation system must be able to satisfy any demands placed upon it for data, and all things being equal, a system with a larger $\mathbf{I_1}$ is better than one with a smaller $\mathbf{I_1}$. One interesting question to be addressed in future experimentation is whether a system with a large $\mathbf{I_1}$ but with a large overall $\boldsymbol{\varpi_\tau}$ is better or worse than a system with a relatively smaller $\mathbf{I_1}$ but also with a relatively smaller $\boldsymbol{\varpi_\tau}$. Additionally, the data transportation system must achieve a small value for $\boldsymbol{\varpi_\tau}$ under all circumstances, because this property will insure that not only can the system handle the data load but that it can also respond to changes in demand rapidly. Some of the values, such as $\mathbf{I_3}$, $\mathbf{I_4}$, and $\mathbf{I_5}$ cannot be altered to a large degree once an organization starts an operation. Therefore, the organization should begin any operation with the capabilities in its data transportation system already present that will allow it to minimize these three values. However, it is clear that $\mathbf{I_5}$ is an important parameter throughout the organization and minimization of this value is an important goal and needs to be pursued via technology and policies. Especially important are modification of policies controlling sensitive but important data; therefore, the need for attaining a small value for $\mathbf{I_5}$ should be a major consideration when considering any policy related to data movement throughout an organization. In order to insure that these values are minimized and because they can be affected only to a small extent once activity begins, simulations of network centric activities where the data needed to compute the metrics outlined here are gathered and analyzed are necessary. Simulations should address as many alternative environments as possible so as to

insure that the data transport system can satisfy the demands that may be placed upon it during the course of an operation. The simulations should, therefore, possess as much fidelity as possible with regard to data transport and the situations simulated should be repeated a sufficient number of times to insure that the results are statistically significant.

7. Summary and Further Work

The US military is undertaking an unprecedented transformation in its movement to a network centric warfighting philosophy, which is characterized by its network capacity and data infrastructure. A network centric force has the capability to share and exchange data among the distributed elements of the force and has access to data whenever and wherever it is needed. The network centric transformation increases the military's reliance upon data superiority and decision superiority, but the policy and doctrinal insights required in order to fully exploit the communication capabilities have yet to be developed. To redress the problem of developing policies that maximize the use of current and future networking and computational resources, we must understand how to translate doctrine and policy into network and computational management policies and how to assess if the policies and doctrine are making the best use of available resources. This paper is a step in that direction, but much remains to be done when the magnitude of the task before us is considered.

Metrics are needed to gain insight into the performance of a C3 configuration. At its root, metrics must enable us to understand the data volume and data velocity capabilities that the configuration provides. Proper metrics allow us to measure the volume of data in transit at any time, the velocity of data movement from source to recipient, timeliness of data arrival, and the handling of priority data; and thereby determine the overall efficiency of information handling within an organization's network centric infrastructure and to determine if the infrastructure and organizational policies promote network centric operations. These metrics combined with additional derived metrics allow us to start to indirectly measure the overall situation awareness of the team or group as well as the ability of the team or group to operate efficiently and process multiple situations simultaneously and effectively. While these metrics do not paint a comprehensive picture of the performance of a C3 architecture, they provide the basis for insight. Our work built upon foundational research, as detailed in many sources such as the NATO Code for Best Practices for Command and Control Assessment, to assemble a set of metrics that can be used to provide new insights into the effectiveness of various C3 configurations.

The network centric paradigm for warfare spans the entire spectrum of conflict, which means that doctrine and policy for the employment of network centric resources that addresses the challenges posed by different types of conflict are required. For example, when performing military planning and operations in a network centric warfare environment, that the operation and use of networks and computational resources will increase in importance. As the use of network centric warfare principles for operational situations increases, the component network and computational applications will become ever more tempting and profitable targets for attack by an enemy. As a result, we must be prepared to address attempts to wrest information superiority from our grasp by reducing our network centric operational capability. Therefore, it is apparent that for NCW to be successful as an operational paradigm into the future, the people who operate within the NCW battlespace must be prepared to deal with attacks upon the network and computational resources that make NCW a viable strategy. In light of this need, operators and information technology specialists must be trained to be able to recognize and counteract a cyber attack against NCW information resources, which is not an easy task. Training environments that accurately simulate the complexity of NCW operations and the elements of a cyberwarfare attack within a NCW environment can be used to prepare to counter cyber attacks against NCW infrastructure, but these environments have yet to be built, the principles to be employed for their assembly have yet to be uncovered, and training methodologies have yet to be developed.

Another important area for future research is to extend the representations presented here. The representations should be extended in the degree of detail they capture and serve as the basis for developing further metrics. In addition, the representations developed here should be extended so that network topologies, bandwidth availability, network attack, and other factors that affect performance in the real world are captured.

An important area of research that must be addressed is the instrumentation of the network and computational resources in order to acquire the data needed to compute the measurements suggested in this paper. To properly instrument the network centric resources, we need to determine where to place the sensors and the data that the sensors should gather. In addition, we must determine how to communicate performance data to a network operations center so that this communication has minimal impact upon the transmission of operational data, maintains efficiency for data transmission, and enhances the responsiveness of the network to changes in load and demand. To achieve these objectives, we believe that research is needed to determine the type(s) of sensors that are

needed, the different means that can be employed to gather the data, and research to assess which approaches to performance data acquisition and dissemination are the most useful and efficient.

An additional area of research that is suggested is refinement of our knowledge about systems engineering and composition when assembling advanced systems of systems to support network centric warfare. We are currently woefully ignorant concerning the factors that influence overall NCW system performance, the key interfaces between NCW systems, the proper placement and priority for development of intelligent aids for routing and releasing data, and how to recognize and adapt to changes in priority of data by various data recipients. In sum, we need to improve our knowledge about the theory and engineering of data transport technologies used in network centric warfare and how changes in components and data priorities affect the overall performance of the data transport system for an organization. Conversely, there is also a need to achieve a better understanding of how data should be prioritized in order to best meet each user's needs in conjunction with the overall organization's needs, ie., how can a user's priorities for data be satisfied without detrimentally impacting the overall performance of an organization's NCW resources. In future work, we intend to explore these and other avenues of research based upon the formulations for NCW metrics and measures presented in this paper.

References

[1] Alberts, D.S.; Garstka, J.J.; Hayes, R.E.; and Signori, D.T. (2001) *Understanding Information Age Warfare*. CCRP Press, CCRP Publication Series: Washington D.C.

[2] Alberts, D.S. and Papp, D.S. (2001) *Information Age Anthology, Volumn 1: The Nature of the Information Age*. CCRP Press, CCRP Publication Series: Washington D.C.

[3] Alberts, D.S.; Garstka, J.J.; and Stein, F.P. (1999) *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Press, CCRP Publication Series: Washington D.C.

[4] Alberts, D.S. (2002) *Information Age Transformation: Getting to a 21st Century Military*. CCRP Press, CCRP Publication Series: Washington D.C.

[5] Alberts, D.S. and Hayes, R.E. (2003) *Power to the Edge* CCRP Press, CCRP Publication Series: Washington D.C.

[6] Command and Control Research Program (2002) *The Code of Best Practices for Experimentation*. CCRP Press, CCRP Publication Series: Washington D.C.

[7] Garstka, J.J. (2000) "Network Centric Warfare: An Overview of Emerging Theory," *PHALANX*, Military Operations Research Society, Alexandria, VA.

[8] Miller, G.A. (1956) "The Magical Number Seven Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *The Psychology Review*, vol. 63.

[9] NATO SAS026 (2003) *NATO Code of Best Practice for C2 Assessment*. CCRP Press, CCRP Publication Series: Washington D.C.

[10] Smith, E.A. (2003) *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. CCRP Press, CCRP Publication Series: Washington D.C.

[11] Webster, S.G. and Gallant, D.S. (2002) "Joint Virtual Battlespace (JVB) Command Control and Communication (C3) Grid," *Fall Simulation Interoperability Workshop*, Orlando, FL, pp. 336.

[12] Alexander, R.A. (2002) "Joint Virtual Battlespace (JVB) – Representing Network Centric Warfare with New and Legacy Simulations," *Fall Simulation Interoperability Workshop*, Orlando, FL, pp. 418-423.

[13] Mathis, T. (2002) "Joint Virtual Battlespace (JVB) Functional Decomposition of Future Combat Systems (FCS) for Modleing, Simulation, and Analysis," *Fall Simulation Interoperability Workshop*, Orlando, FL, pp. 555-565

[14] Snively, K.; Wilson, A.; and Wuerfel, R. (2002) "Large-Scale Federation Design for JVB Using the RTI-NG," *Spring Simulation Interoperability Workshop*, Orlando, FL, pp. 734-743.

[15] Turrell, C.; Igarza, J.L.; Renda, F.; Brown, R.; Pixius, K.; and Rouget, C. (2003) "Federation Development and Execution Process (FEDEP) Tools in Support of NATO M&S Programs,: *Spring Simulation Interoperability Workshop*, Orlando, FL, pp. 385-391.

[16] Tolk, A. (2001) Integrating NATO M&S Efforts and NATO C3 Technical Architecture, *2001 European Simulation Interoperability Workshop*, Harrow, UK, pp. 607-620.

[17] Tolk, A. and Huber, R.K. (2002) "NATO Code of Best Practices for C2 Assessment – Implications for SISO," *Spring Simulation Interoperability Workshop*, Orlando, FL, pp. 39-48.

[18] Falzon, L.; Davies, M.; Burgess, G.; and Gabrisch, C. (2002) "Behavioral Representation Challenges in Theatre-Level Planning Support," *2002 Conference on Computer Generated Forces and Behavior Representation*," Orlando, FL, pp. 403-410.