

## **Information Command and Control**

**H. Bennett Teates**

Johns Hopkins University Applied Physics Laboratory  
1100 Johns Hopkins Road  
Laurel, MD 20173  
Phone: 240 228 5705  
Email: [Bennett.Teates@JHUAPL.edu](mailto:Bennett.Teates@JHUAPL.edu)

## Abstract

While information has always been the substance of which command and control is made, it has become the thumbscrew of current military, business, and political strategy and operations. From the military perspective, information has become the centerpiece of net-centric warfare and as such has, in essence, become the most recent, fifth, military domain. (1) For the four older, previous military domains, we have developed methods and means to wage war and to command and control what we call the kinetic space. But so far we have developed little to no methods or means of providing the decision-maker a capability to command and control the new domain of warfare, the information space. This paper attempts to raise the level of awareness regarding the need for information command and control (IC2) by addressing some critical challenges surrounding IC2 and offering some insight to fledgling research that attempts to begin meeting these challenges.

It is worthy to note from the start that the purpose of this paper is not to offer the solution, but rather to raise the level of awareness and to suggest some approaches to the need described.

## Introduction

The reason for existence of the military transformation toward net-centric warfare is the perceived value of fully shared information in achieving decision cycle dominance. Even though information has always been important to warfare, our technological capability to collect, process, store, manipulate, retrieve, display and communicate information has evolved and recently matured to where we now consider information as being the fifth domain of warfare. As such it comprises not only information in warfare, but also information as warfare.



**Figure 1 Evolution of the Five Military Domains** Source: GEIA

In moving toward a net-centric war fighting capability, it is generally accepted that obtaining and maintaining a common perception of the situation is essential to a

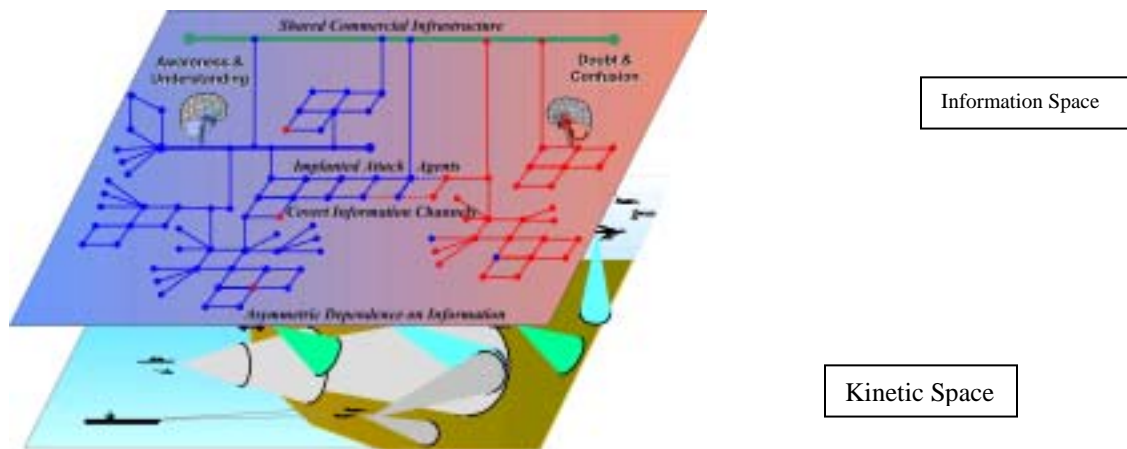
coordinated, cohesive fighting force; one that can, by knowing the commander's intent and the situation, respond with minimal additional command and control. This need for a common perception of the situation has resulted in specific programs to develop the Single Integrated Air Picture (SIAP), the Single Integrated Ground Picture (SIGP), the Single Integrated Maritime Picture (SIMP), and the Family of Integrated Operational Pictures (FIOP). The Single Integrated Space Picture (SISP) has been around since the founding of NORAD. So what is missing from this picture (no pun intended)? Namely, the key to the whole enchilada - no Single Integrated Information Picture- the stuff which will make or break net-centric warfare!

To get to the point of being ready to present a Single Integrated Information Picture (SI2P), we need to first take a look at information in general.

### Relevance to C2

Given that network centric warfare is predicated upon the ability to create and share high level awareness and to leverage this shared awareness to rapidly self-synchronize effects, then the ability to have awareness of information sources, access, paths, and users, both friendly and enemy, is mandatory. It follows, therefore, that the ability to have command and control (C2) of information is essential.

Just as C2 has been applied to the kinetic “space” of war since war's inception, C2 must be now applied to the information “space”.



**Figure 2 The Information versus the Kinetic Space**  
(Copyright JHU/APL. All rights reserved. Reprinted with permission. Not to be used or duplicated in whole or in part without permission of JHU/APL.)

Knowing the status of one's information systems versus the status of the enemy's information systems places the “transformed military commander” in a “playing field” tilted in his favor. Indeed, knowing the status of both friendly and enemy information systems provides the knowledge to defend one's own system and to effectively attack the other's system.

Interestingly, as practitioners, investigators, and integrators of technologies and systems to support C2 with better and better information capabilities, we have reached the point where information, itself, is a capability requiring C2. In the commercial world,

recognition of information as key to an entity's continued, profitable existence has resulted in the organizational specialty of Chief Information Officer (CIO). This led to the Clinger-Cohen Act that resulted in all Federal agencies having CIOs as well. Even so, it is interesting to note that we are this far into the Information Age and don't have methods or means to value information. Several years ago, RADM Grace Hopper made the observation, *"Some day on the corporate balance sheet there will be an entry which reads: 'Information;' for in most cases the information is more valuable than the hardware which processes it."* While this quote is becoming truer with each passing day, industry has not yet put information as an asset on its balance sheets. (2) Perhaps the military can lead the way!

### **The Value of Information**

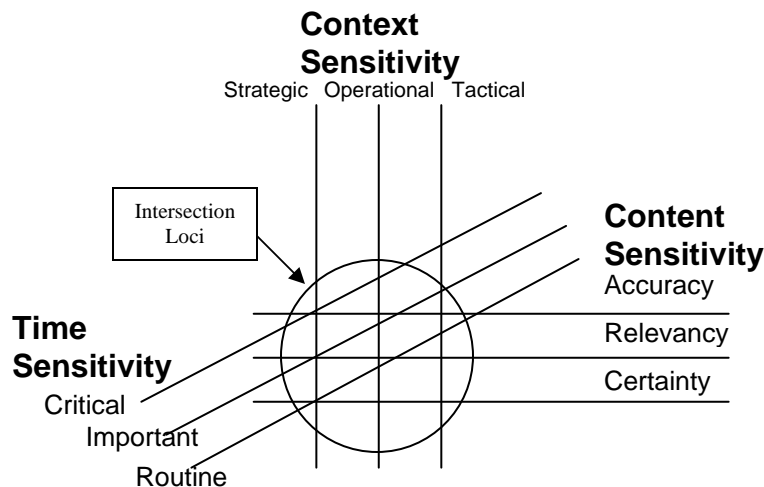
We can and have developed systems that can collect, communicate, and store information. We can and have developed systems to assure information being used is the same as information collected (integrity). But we have not developed a means to value information and then to keep up with its changing value.

Using information effectively requires:

- Knowing it exists
- Knowing where it is located
- Having access to it
- Believing it to be valid
- Knowing how to use it
- Knowing its value

The key to IC2 is to be able to get a handle on the value of information. If you do not know what a pound of information is worth, then you cannot manage what you cannot measure. How will we achieve information superiority if we don't know the value of information? How will we be able to exploit the fifth domain of warfare if we don't know how to value our information or that of our adversaries? C2 of the kinetic space uses the value of physical assets to make decisions. C2 of the information space must use the value of information to make decisions, as well. But the value of information changes with the situation. The value of information is dependent upon its content, its context, and its timeliness. (3)

One approach to framing information is to see it as a multidimensional entity, controlled by time sensitivity (Critical, Important, Routine), context sensitivity (Strategic, Operational, Tactical), and content sensitivity (Accuracy, Relevancy, Certainty). Figure 3 illustrates these dimensions and the loci of their intersections. Since these dimensions are in constant flux, it becomes necessary to find a way to present these dimensions to the commander so that he has a quick and intuitive understanding of his information space.



**Figure 3 Multidimensional Approach for Determining the Perceived Value of Information**

### Information Visualization

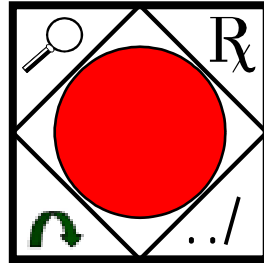
Net-centric warfare will generate increasing amounts of information and for the commander to be capable of assimilating this information and providing a Single Integrated Information Picture (SI2P) requires approaches involving visualization. Visualization is only one aspect of a broader range of methods of perceiving and assimilating information. Haptic (touch) feedback is beginning to see use in specialized applications, and the use of audio is becoming more common. However, people perceive information primarily through vision, and the display of information is likely to continue to be designed primarily for visual perception.

Information visualization enables the commander to deal with all of this information by taking advantage of our innate visual perception capabilities. By presenting information visually, it is possible for the human brain to use more of its perceptual system in initially processing information, rather than immediately relying entirely on the cognitive system. Information visualization applications rely on basic features that the human perceptual system inherently assimilates very quickly: color, size, shape, proximity, and motion. Because each feature can be used to represent different attributes of information, good visualizations enable us to not only perceive information more easily, but also to perceive more information at one time. We can immediately see patterns in information that indicate trends, recognize gaps, discover outliers or errors, pinpoint minimum and maximum values, and identify clusters. As a result, information visualization applications enable us to better understand complex systems, and make better, faster decisions.

The value of information that is proposed above is multi-dimensional (there are three dimensions discussed above; more dimensions will be discussed later), and techniques have been developed to visualize multi-dimensional data. (4)

However, for the moment, consider visualization of the loci illustrated in Figure 3 by using the color spectrum (blue equal to cool through red equal to hot). A circle displaying a color from blue to red might be used as one approach to displaying

information value, where blue is low value, green is of some greater value, yellow is of even more value, and red is high value. White is no information available. Figure 4 illustrates this approach by what we have termed the Information Value Cell (IVC).

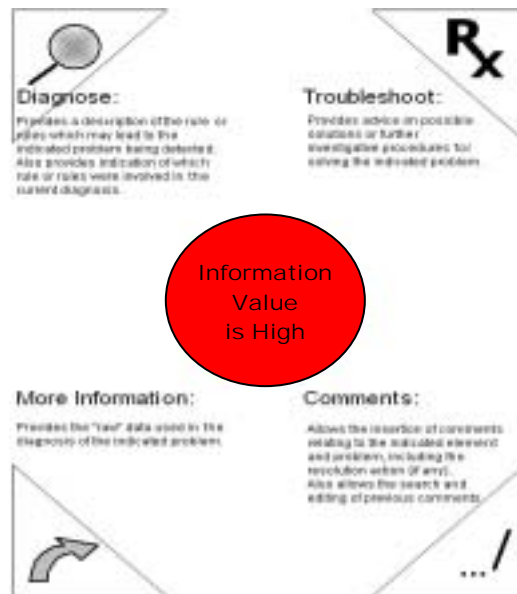


**Figure 4 Information Value Cell Visualization**

(Copyright JHU/APL. All rights reserved. Reprinted with permission. Not to be used or duplicated in whole or in part without permission of JHU/APL.)

The IVC links to the underlying constituent parts through the icons illustrated in each corner of the Information Value Cell as explained in Figure 5.

The Information Value Cell can be augmented with explanatory and decision-making assistance as follows:



**Figure 5 Retrievable Detail About an Information Value Cell**

(Copyright JHU/APL. All rights reserved. Reprinted with permission. Not to be used or duplicated in whole or in part without permission of JHU/APL.)

While an intuitive understanding of information value is important to a commander, a more rigorous approach than perceived value to make decisions and allocate resources is clearly necessary. A formula like this is one approach:

**Formula 1:** Information Value =  $\{[(Wt1Wt2Wt3) (\text{attribute } 1)] + [(Wt1Wt2Wt3) (\text{attribute } 2)] + \dots\}$

Where: Attributes are based on mission (value, risk, cost, effect, etc.)

Weights are based on content, context, and timeliness (they also include information assurance weights, as in Figure 9)

Hence, for example, an Information Value of 90 to 100 would be color-coded as red in the Information Value Cell; a value of 80 to 90, yellow, etc. Both attributes and weights may be the result of subject matter expertise, models/simulations, and/or probabilities derived from statistics, neural nets, genetic algorithms, etc.

### Mission Centric Operations: An Example of Information in Warfare

The End-to-End Global Information Grid (GIG) is the future implementation supporting Network Centric Operations and Warfare (NCOW) in the DoD spanning each of the Joint Forces' Transformation Roadmaps. Figure 6 illustrates the logical view of networks that will span from the national to the tactical levels. (5)

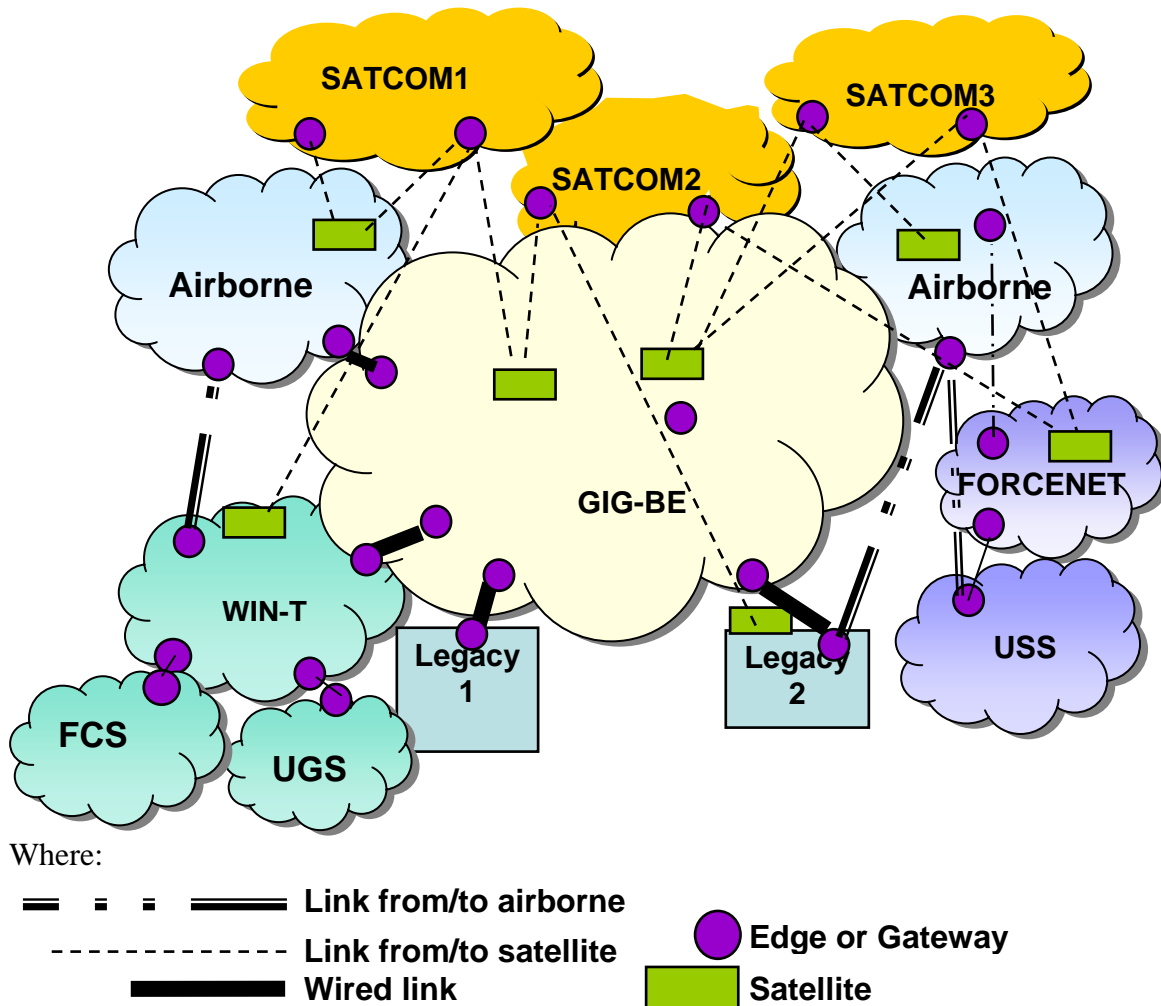
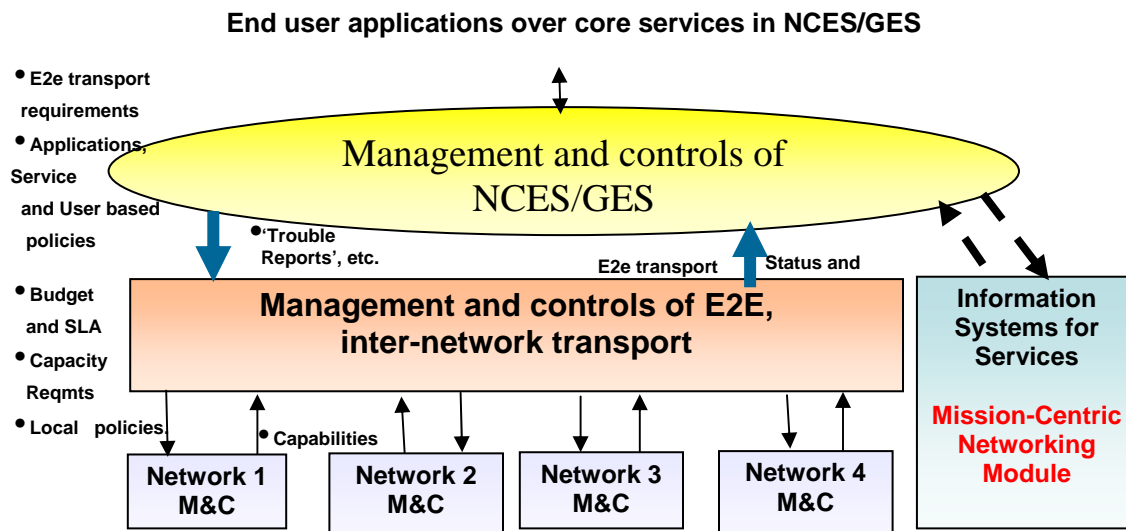


Figure 6 Illustration of the GIG Networks

However, these networks, that will enable dominance across the entire mission landscape, will exceed the capabilities of network operators. Real time, mission-focused allocation of GIG resources to support NCOW requires that the GIG itself must constantly be aware of real-time information activities. To manage this array of networks and information a schema that might be used is illustrated in Figure 7. (5)



### Figure 7 An Illustrative Schema for Managing the GIG

The hypothesized Mission-Centric Networking Module (MCNM), illustrated in the Information Systems and Services Function in Figure 7, would provide real-world awareness that enables the end-to-end GIG to effectively support its many constituent networks and applications. (6) But this Module will depend upon knowing the value of information to make real-time decisions regarding the dynamic use of resources.

The MCNM should be a networked operations system that monitors network activities, generates and maintains situational awareness of operational activities, and uses this joint situational awareness of network and operational activities to predict the mission impact of alterations and disruptions of networked resources. The MCNM should use a predictive capability to rank corrective network-operation courses-of-action (COAs) and interpret network alarms in terms of expected operational mission impact. (3) This capability depends on knowing the value of information as generally defined above and begs the need for Information Command and Control (IC2). Figure 8 illustrates how this information situational awareness might be visualized for use by the commander.

Network and operational commanders could use the MCNM to monitor and comprehend how their networks are supporting various missions and how actions taken on their networks will affect their missions. The risk of not using a MCNM-like capability is that network resource allocations and/or corrective network decisions will likely be made



without foresight which could lead to inappropriate network management decisions that could cripple net-centricity and mission effectiveness.

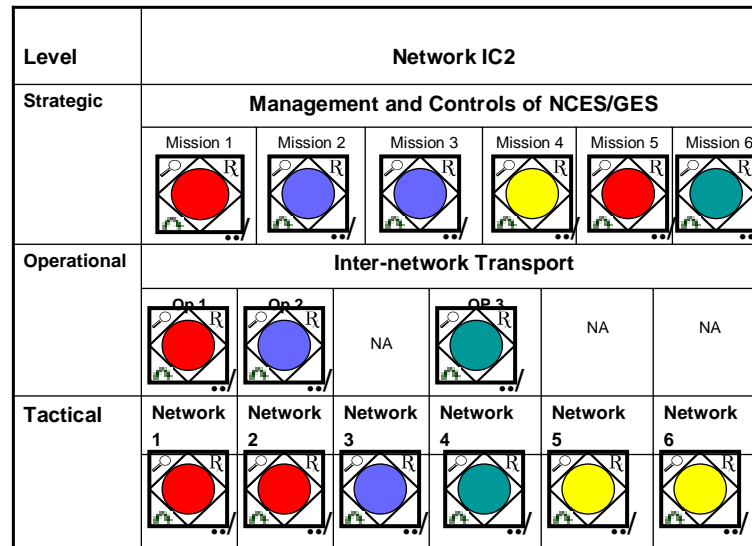
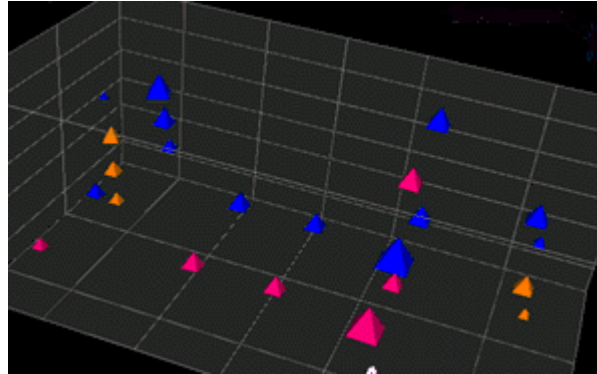


Figure 8 A Possible IC2 Visualization for GIG Management

The MCNM envisioned could offer significant functionality not available in network monitoring tools currently used by the Network Managers (e.g., “HP OpenView™” or “What’s Up Gold”) that simply monitor levels of subsystem performance to determine problems with network devices or connections. Current network monitoring tools do not report the implications of network health on the viability of the supported missions, and current tools provide their users with scant means of predicting the effect of network-operation COAs on operational activities.

The MCNM would take advantage of the fact that information networks are more than just a means of transporting data; they are themselves a sensor in their own right, providing critical insight into the status of operations and the role that information plays in support of those operations. (7)

Another approach to visualization of these values is to apply the Information Value Cell results to a three-dimensional view, generating an Information Value Space. Figure 9 provides an example of how this visualization might be used to aid the commander in the use of information.



Source: Applied Visions, Inc

Figure 9 Illustration of an Information Value Space

### **Cyber-Centric Operations – An Example of Information as Warfare**

In today's Information Age, we must become concerned with the "misuse" of information as well as its use. The old saying, "knowledge is power" is even truer if someone else holds your information as their knowledge! Indeed, the whole new world of Information Operations is about defending one's information from adversarial knowledge and actions while at the same time using one's adversary's information and information systems against him.

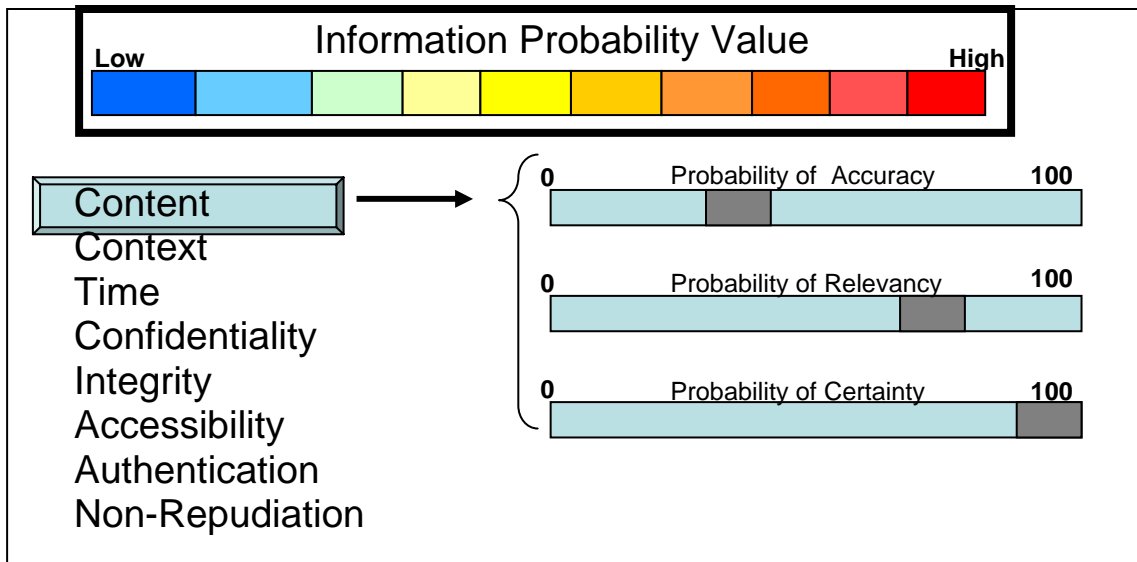
Information as warfare may take one or a combination of the following examples:

- Network analysis and exploitation - the ability to covertly analyze networks of the adversary to prepare for their penetration to steal their information if and when needed
- Cryptographic protection and exploitation – the encrypting our and ally information so it is unreadable by any who have no need to know, and the decrypting of adversaries' information
- Hunter killers – software agents that search the Internet, identify the adversary's nodes, deny them the use of these nodes, and inject disinformation, worms, and viruses
- White cells – software agents that attach themselves to malicious code in our nodes and render their code useless

There are others, but even to develop these and use them in defense of our own networks or in attack of adversarial networks requires placing a value on information. This mode of information use must be valued, in addition to the dimensions discussed above, along several new, additional dimensions; namely, integrity, confidentiality, accessibility, authentication and non-repudiation. These dimensions comprise what is called Information Assurance (IA).

As Formula 1 is scalable, adding these dimensions to the estimate of information value provides a means to visualize our and our adversary's information systems to better allocate resources for protection in our case and/or attack in the other's case.

It is worthy to note that Formula 1 as presented here is completely static; contains no dynamic state variables, and will provide only the coarsest description of any value of information. Figure 9 illustrates a method to allocate probabilities to each attribute and derive a composite value for information. Automating a schema like this may provide a means to maintain a dynamic visualization of information value.



**Figure 10 Illustration of Multi-dimensional Derivation of Visualization of Information Value**

Again, the value of this information can be represented by the Information Value Cell of Figure 4 or the Information Value Space of Figure 9.

## Summary

The issue of Information Command and Control (IC2) requires (to name a few) theory, definition, scope, assessment methods, and practice. Just as C2 in general needs a basis for measurement and value, IC2 requires a basis for assessing and visualizing informational value. This paper has outlined an approach to developing a value for information and for visualizing this value in an Information Value Cell (IVC). Collections of IVCs can be used to present a Single Integrated Information Picture (SI2P) and an Information Value Space (IVS) for a common understanding of information within a unit or force. Examples of the use of the IVC and IVS are discussed in applications to information in warfare and information as warfare, respectively. The value of information in warfare is presented as a function of context, content, and time. It is illustrated in a mission-centric context to show its value in managing information networks within the GIG.

The value of information as warfare is presented as a function of information assurance (IA) attributes. It is discussed in a cyber-centric context to show its value in preparation of the information space so that commanders' decisions regarding the collection, denial, discombobulation, use, and/or pathways of our and our adversaries' information can be prioritized for protecting (in the case of our cyber systems) and attacking (in the case of the adversary's cyber systems).

## **Conclusion**

It is concluded, just as begun, that much work remains to be done to develop a standard, correct, and acceptable (yet pragmatic) means to assign measurable value to the information supporting the warfighter. Information value is critical, and to manage the montage of information systems that support warfighters, these information value metrics need effective visualization. Such visualization will likely rest upon yet-to-be developed abstractions that correlate the flow of information to its expected impact on the operational activities in which the warfighter may be engaged. An operational awareness within the network management system that includes mission status and sensitivity of ongoing mission activities to information flows and value is needed. No more will the focus be on how to configure bandwidth pipes and straws in the false hope that we can get all the information to everyone, everywhere; there are always constraints. Rather, the focus will be on how to move that information which maximizes effectiveness on operations.

While this paper describes some approaches, its primary purpose is to raise the issue of why Information Command and Control is needed if net-centric warfare is to fulfill its promise and enable the Joint Vision 2010 goal of Information Superiority.

## **Acknowledgements**

The work presented in this paper has been prepared "on the shoulders" of seminal work done by many others. In particular I would like to acknowledge George Barrett and Mike Hostetter of the Johns Hopkins University Applied Physics Laboratory and Perry Luzwick (Reference 3) of Northrop Grumman.

## **References**

- (1) Government Electronic Industries Associate, "Economic IT DoD Forecast", 2001
- (2) Daniel Moody, Peter Walsh, "Measuring the Value of Information: An Asset Valuation Approach", European Conference on Information Systems (ECIS), 1999
- (3) Andy Jones, et al., "Global Information Warfare", CRC Press, LLC 2002
- (4) Gary Geisler, "Making Information More Accessible: A survey of Information Visualization Applications and Techniques", Jan. 1998
- (5) Doshi, B; Jones, S: et al, Independent Research and Development White Paper, Johns Hopkins University Applied Physics Laboratory, 2004
- (6) Pistole, J. and Barrett, G., "Mission-Centric Networking Module", JHU Applied Physics Laboratory internal report RTDC-TPS-447 (2003).
- (7) Barrett, G. and Lee, S., "Mission-Centric Network Defense System", U.S. Patent Application 10/679,606. Patent Pending, Johns Hopkins University Applied Physics Laboratory.
- (8) Applied Visions, Inc. , Secure Scope™, "How Does 3-D Visualization Improve Security Decisions", ([www.securedisions.com](http://www.securedisions.com)), 2004

**Bibliography**

H. Bennett Teates is currently a senior program manager at the Johns Hopkins University Applied Physics Laboratory (JHU/APL), addressing development of command, control and communications systems for net-centric warfare and the Unified Enterprise Command Structure (UECS). Prior to joining the JHU/APL he was the co-founder and CEO of Command Control, Inc., in Atlanta, Georgia, where he led the development of command and control applications for both the military and industry. He is the author of several papers and a book chapter dealing with command, control, and communications. He holds a B. Sc. degree in Electrical Engineering for Virginia Tech and advanced degrees from the George Washington University and the Johns Hopkins University. His work toward a Ph.D. was conducted at Georgia State University in Decision Sciences.