MP05B0000043

MITRE PRODUCT

Enterprise Systems Engineering Theory and Practice

Volume 9: Enterprise Research and Development
(Agile Functionality for Decision Superiority)

February 2006

Dr. Kevin A. Cabana
Dr. Lindsley G. Boiney
Mr. Robert J. Lesch
Mr. Christopher D. Berube
Dr. Lewis A. Loren
Ms. Linsey B. O'Brien
Mr. Craig A. Bonaceto
Mr. Harcharanjit Singh
Mr. Robert L. Anapol

Sponsor: MITRE
Dept. No.: D400
Contract No.:
Project No.: 03AAV400-C2

MITRE
Center for Air Force C^2 Systems
Bedford, MA

Preface

This is the ninth in a series of preliminary volumes that define and examine key building blocks of the evolving field of Enterprise Systems Engineering:

Volume 1: Enterprise Characteristics and Challenges
Volume 2: Systems Thinking (New and Emerging Perspectives)
Volume 3: Enterprise Architecture (Application Across the ESE Spectrum)
Volume 4: Enterprise Management (Processes to Bridge Theory and Practice)
Volume 5: Enterprise Opportunity and Risk
Volume 6: Enterprise Activities (Evolving Toward an Enterprise)
Volume 7: Enterprise Analysis and Assessment
Volume 8: Capabilities-Based Planning Analysis
Volume 9: Enterprise Research and Development (Agile Functionality for Decision Superiority)

The volumes are intended as guidance for researchers and practitioners who are expanding from a Traditional to an Enterprise Systems Engineering paradigm. Topics for examination include: the complex characteristics and behaviors of enterprises, the challenges these pose for engineering practice and technology development and application, and the impacts of leading-edge technologies on enterprise goals and objectives, to better gauge associated risks, opportunities, and potential.

Abstract

Volume 9 lays the groundwork for the D400 Enterprise Systems Engineering Research and Development paradigm. Motivating our paradigm is a fundamental goal of Network-Centric Warfare and Operations (NCOW): "getting the right information to the right people at the right time to make the right decisions." To contribute to the realization of this goal, we have identified agile information generation, management, and exploitation as the three canonical function areas that underpin our paradigm. Information generation addresses the problem of "getting the right information" by collecting, fusing, aggregating, and drawing inferences from data gathered from any and all sources on the extended battlefield—and in a network-centric world, any entity that can make observations can function as a data-generating sensor. Information management addresses the critical need of constructing sufficient infrastructure to ensure that this information is made available to "the right people at the right time, constrained by the right budget" in the highly distributed and fluid force of the future. The primary focus of information exploitation is the combination of people and technology to process this information to make "the right decisions." Our paradigm addresses the agile, flexible combination of these functions across multiple enterprise scales and military echelons for both the conventional and asymmetrical threats that characterizes the 21st century security environment.

An important aspect of the paradigm is that warfighters and their mission areas are the "forcing function" for the development of information technology and collaborative processes that serve to promote innovation in decision making. Within this framework, we recognize that a large part of enterprise complexity comes from the fact that its performance and evolution are driven by creative and adaptable people interacting with systems, organizations, and external influences. Identifying both positive and negative effects of this "emergence" is an important research goal.

Section 1 motivates the need to transform the military into a network-centric enterprise, describes the defining characteristics of this enterprise, and summarizes key building blocks of the research paradigm. Sections 2 through 4 describe information generation, management, and exploitation in greater detail by highlighting the critical design principles and research needs to ensure their agile combination. To highlight anticipated returns-on-investment from this research, Section 5 considers a complex, time-sensitive operational scenario in which all three functions of the paradigm come together fluidly to improve military effectiveness and impact.

Table of Contents

List of Figures

List of Tables

1 Overview

Introduction

This volume lays the groundwork for the D400 Enterprise Systems Engineering Research and Development paradigm. Motivating our paradigm is a fundamental goal of Network-Centric Operations and Warfare: “getting the right information to the right people at the right time to make the right decisions”, under the highly complex and dynamic challenges of 21st century warfare. To contribute to the realization of this goal, we have identified the canonical functions of information generation, management, and exploitation, and their agile combination, as major building blocks of our research paradigm. The Oxford English Dictionary defines agile as “having the ability to move quickly and easily” (Simpson & Wiener, 1989). Achieving agility in dynamic military and security environments requires flexibility, i.e. “the ability to change in response to new and different circumstances” (Simpson & Wiener, 1989). Portions of the enterprise, or subsets of people, systems, and processes within which these functions operate, must be able to reconfigure themselves in new and unanticipated ways to rapidly support military objectives under changing and uncertain scenarios. At the highest level, the enterprise must be robust, or able to withstand change without serious impact to its support of military effectiveness, or its ability to evolve to provide new and better capabilities.

In the 21st century security environment, information generation addresses the problem of “getting the right information” by collecting, fusing, aggregating, and drawing inferences from data gathered from any and all sources on the extended battlefield—and in a network-centric world, any entity that can make observations can function as a data-generating sensor. Information management addresses the critical need of constructing sufficient infrastructure to ensure that this information is readily available to “the right people at the right time constrained by the right budget” in the highly distributed and fluid force of the future. The primary focus of information exploitation is the combination of people and technology to process this information and make “the right decisions” in time-sensitive and unpredictable environments. The agile combination of information generation, management, and exploitation is hypothesized to promote the fluid application of combat power, enabling it to move quickly and easily where it is needed. In our paradigm, information technology exists to serve the needs of the warfighter, and we acknowledge that a large part of enterprise complexity comes from the fact that its performance and evolution are driven by creative and adaptable people and teams, functioning across organizations, cultures, military echelons, and enterprise scales.

In this introductory section, we begin by addressing the current and future state of warfare and how it has driven the military to transform itself into a network-centric enterprise to establish and maintain a decisive edge over our adversaries. This transformation has broad and deep implications for our research and development paradigm, forcing us to consider how to engineer an agile enterprise in such environments. Our paradigm is based in the integration of leading-edge technologies such as cognitive science, complex adaptive systems – including biologically-inspired methodology, and enterprise systems engineering, with classical approaches from information technology and distributed computing. We go on to consider characteristics of the Command and Control (C2) Enterprise and how, within the above integrative framework, our canonical functions can serve to enable enterprise capabilities. The remainder of this volume describes characteristics that underpin the agility of information generation, management, exploitation and their combination in greater detail by highlighting key challenges, engineering design principles, and research needs within and across these areas. The final section of this volume describes a complex and time-sensitive operational scenario in which all three functions of the paradigm come together as hypothesized to improve military effectiveness and impact.

Motivation: The Future of Warfare

Throughout history, warfare has always been a complex and messy undertaking. Twenty-first century warfare is proving to be even more complex, with multi-dimensional challenges to U.S. global interests across a spectrum of conflict never before experienced. There is no clearly defined battlefield – rather, the battlespace is global, stretching to wherever we have interests and vulnerabilities that can be attacked or exploited by our adversaries. There will of course continue to be traditional force-on-force warfighting, but it will be very different and likely to be conducted alongside humanitarian missions, peacekeeping activities, and responses to asymmetrical threats like the current insurgency in Iraq and the global war on terror, where our adversaries will fight us on their terms with a range of effective and unforeseen techniques, based on complex human and social networks with clear "commander's intent" (Hanifen, n.d.). These techniques can often negate our technological advantages and challenge our will to continue (Potts, 2003). Figure 1 depicts a snapshot of some of the challenges and complicating factors we continue to face as our adversaries evolve.

Figure 1: The twenty-first century warfare environment[1]

From this emerge three key aspects of the future warfighting environment with significant implications for the United States and its coalition partners:

1. We will continue to have global interests and be engaged with a variety of regional actors. The joint force of the future must be prepared to achieve victory across the full range of military operations in any part of the world, to operate with multi-national forces, and to coordinate military operations as necessary with government agencies and international organizations.

2. Potential adversaries will have access to the global commercial industrial base, the global commercial infrastructure, and much of the same technology that we possess. We will not necessarily sustain a wide technological advantage over our adversaries in all areas. Our advantages must therefore come through improvements in concepts of operation, doctrine, organizations, training, education, leadership, and force structure that collectively enable us to take full advantage of technology to achieve superior warfighting effectiveness (Alberts, 1996). And we will need to iterate through these improvement and adaptation cycles more quickly than our adversaries.

[1] From Hanifen, n.d.

3. As our capabilities evolve, we should expect potential adversaries to adapt and make use of asymmetric approaches that avoid U.S. strengths and exploit potential vulnerabilities, such as attacks against U.S. citizens and territory.

Response: Military Transformation

The comprehensive response to this future warfighting environment is the transformation of the military into a joint force that is dominant across the full spectrum of military operations, that is: persuasive in peace, decisive in war, and preeminent in any form of conflict. This is tantamount to an endorsement of a broader and not always conventional vision for how U.S. military power should be applied, that recognizes that the military will likely be involved in humanitarian and peacekeeping missions, while also being called upon to respond quickly to imminent security threats. For the joint force of the future, these goals will be accomplished through a doctrine of Full Spectrum Dominance--the ability of the military, operating unilaterally or in conjunction with multinational and interagency partners, to defeat any adversary and control any situation across the full range of military operations (Hanifen, n.d.). Figure 2 shows some of the key enabling concepts for Full Spectrum Dominance.

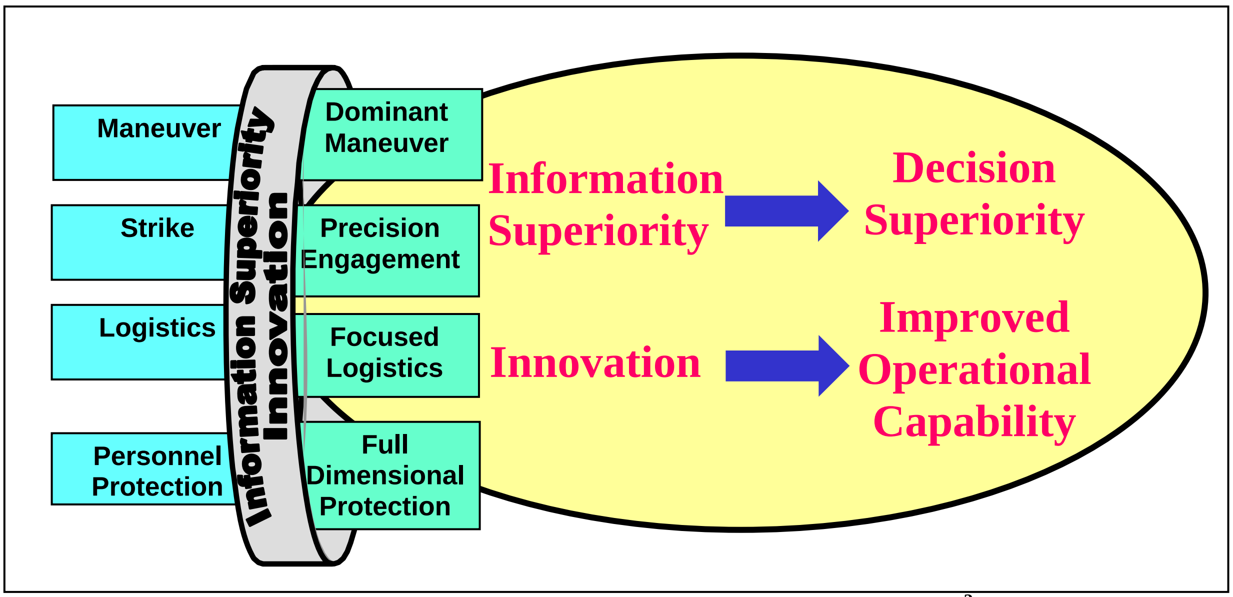

Figure 2: Enabling concepts for Full Spectrum Dominance[2]

To make this transformation highly adaptive to the type of asymmetrical threat that characterizes insurgents, terrorists, and other non-state actors, this vision must be extensible to an emerging concept of maneuver warfare spearheaded by the Marine Corps, Distributed Operations, where a military configured as small, highly skilled and independently-operating units can aggregate quickly to apply sufficient and just-in-time force wherever it is required

[2] From Hanifen, n.d.

against a complex and adaptive threat. This threat is fueled by strong social networks and timely, pervasive human intelligence to leverage dispersed attacks that result in chaos, friction, and uncertainty. Without access to equivalent social networks and human intelligence, our response must be based on greater support from technology, collaborative tools, and processes that provide our forces with timely situational awareness to make and execute decisions across military echelons - with the full power of the enterprise behind these decisions. The D400 research and development paradigm detailed throughout this volume is a dedicated, albeit modest attempt to address this asymmetrical need while providing greater flexibility for our response to more conventional threat. Capabilities needed to support Distributed Operations can be summarized as: (1) the ability for dispersed, maneuvering forces to conduct network-enabled operations and make critical, real-time decisions, (2) increased situational awareness for ground forces, based on timely and sufficient (rather than optimal) information, (3) the sustainment of widely dispersed units over extended periods, and (4) enhanced individual and collective mobility of ground forces (McBrien, 2005). Our research and development efforts must therefore be extensible to these capabilities, while serving to provide greater agility to the more centralized and hierarchical demands of time-sensitive team decision making for conventional warfare.

Engineering the C2 Enterprise

The primary challenge for this transformation is the engineering of a powerful Command and Control (C2) Enterprise, characterized by the complex interaction of people (e.g., soldiers, commanders, systems engineers), processes (e.g., doctrine, concepts of operation, rules of engagement, information sharing practices), and technologies (e.g., information systems, decision support systems, weapons systems, sensor systems), that interact with each other and their environment to achieve organizational goals such as decision superiority. Figure 3 shows the graphical depiction of a notional enterprise that is highly recursive, and comprised of many sub-enterprises, each constituting an enterprise at its own level. For the C2 Enterprise, the Airborne Warning and Control System (AWACS) constitutes its own enterprise, and it is likewise comprised of sub-enterprises of people, processes, and technologies with their own "local" goals and functions which in turn serve the enterprise-wide goals and functions. This recursive nature of the C2 Enterprise adds to its complexity and demands new ways of engineering, shaping, modeling, and understanding these systems and relationships to effectively achieve its organizational goals. The emerging field of Enterprise Systems Engineering embodies the framework necessary to promote this change.

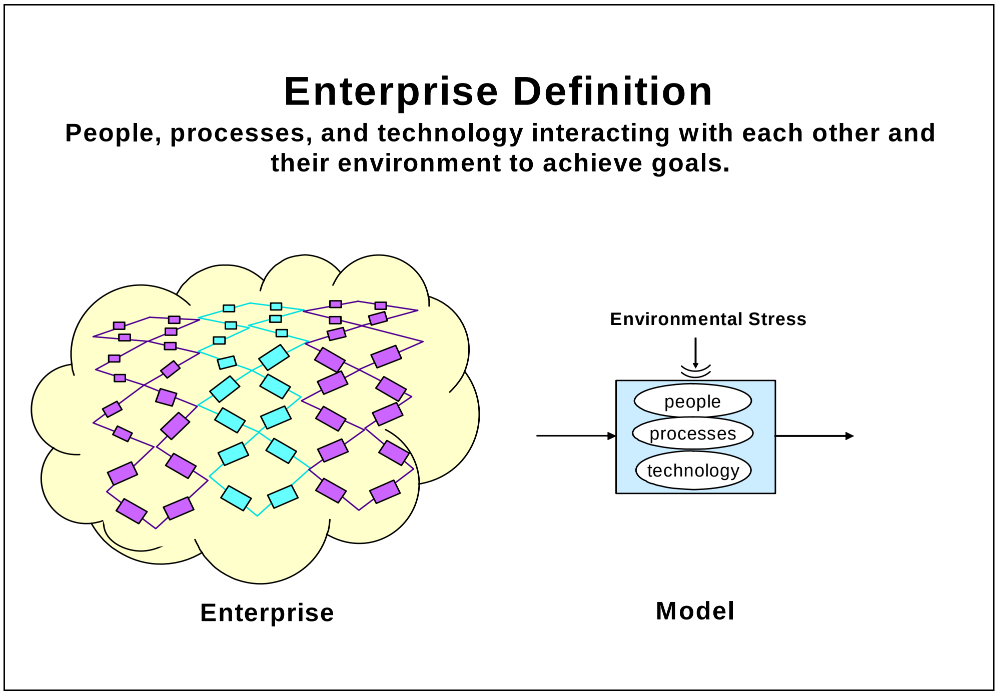

Figure 3: A notional enterprise

A related and important feature of an enterprise is its dynamism. That is, an enterprise is in a constant state of evolution, reinventing parts of itself through a process of continual innovation and integration. As enterprise systems engineers, we must shape the integration and innovation environment so that the target capabilities are better able to be envisioned and maintained. A particular challenge for researching and developing these capabilities, derived from this characteristic, is the need to work fluidly and transparently across multiple scales of an enterprise.

To illustrate the evolutionary nature of an enterprise as it adapts itself to new goals and constraints, consider the military problem of resource allocation, where a limited number of assets (e.g., weapons, tankers) must be paired against a number of objectives (e.g., targets, aircraft in need of refueling) to achieve mission goals and make the best use of these assets. One way to solve this problem would be to develop a system tailored to a specific resource allocation problem. Such a system would be incapable of adapting itself to other and perhaps unforeseen resource allocation problems. As an alternative approach, consider instead a family of generic resource allocation algorithms and visualization techniques that exist on the enterprise and could be applied to a myriad of resource allocation problems. Such components could be rapidly adapted and reconfigured to meet the demands of any resource allocation problem. Moreover, operators trained in resource allocation decision-making could rapidly apply these skills to different areas as the demands of conflicts shift. Such an approach is highly consistent with our vision of an agile enterprise comprised of a variety of adaptable components that can be rapidly reconfigured to meet changing demands, and for which the line between systems acquisition and systems operation is continually “blurred” by humans who constantly adapt themselves and their systems to meet the emergent challenges of warfare.

Important leading-edge disciplines that serve as foundational elements of Enterprise Systems Engineering include:

1. **Complexity Theory (Complex Adaptive Systems)**

   The C2 Enterprise is a Complex Adaptive System, comprised of many people, processes, and technologies that interact with each other in ways that continually reshape their collective future. The interactions and connections among these diverse elements lead to emergent features (which may or may not be desirable or predictable), and reflect the enterprise tenet that “the collective whole is greater than the sum of its parts.” Because our adversaries also function as Complex Adaptive Systems (in many instances co-evolving with our own), both research and engineering practice need to work to understand where the leverage points are in Complex Adaptive Systems so that we can harness complexity and use it to our advantage (Axelrod & Cohen, 2000) – and to the disadvantage of our adversaries.

2. **Social Science and Social Network Theory**

   In the C2 Enterprise, people do not work in isolation. Because of this, we need to understand the dynamics of team collaboration, distributed decision making, information sharing, trust formation, and the development of shared situational awareness. As we move to joint and coalition military and cross-agency venues, we need to understand how to overcome the social and cultural barriers that hinder effective cooperation.

3. **Cognitive Science**

   People are ultimately responsible for making decisions and taking actions in Command and Control. To serve this, we need to understand their decision-making and cognitive strategies, their biases, how they build and maintain situational awareness, and their performance limits. Ultimately, we need to engineer effective support systems and infrastructure to aid them in meeting their decision-making goals.

4. **Information Science**

   Information is the lifeblood of the C2 Enterprise. We need to understand how to best leverage information technology, in conjunction with the above (and other) disciplines, to generate, manage, and exploit information in a manner that provides us with a continual edge over our adversaries.

Network-centricity: The Hallmark of the Next Generation C2 Enterprise

The C2 Enterprise will continue to mature and evolve as a complex collection of people using processes and technology to achieve their objectives. To a progressively greater extent, these enterprise “agents” will not be located in only one place. Thus, in order to make the best use of this geographical dispersion, these forces must be able freely share, exchange, and exploit information to address any level of threat (Alberts, Garstka, & Stein, 1999). This key principle of Network-Centric Operations and Warfare (NCOW), the Concept of Operations for the C2 Enterprise, is summarized in Figure 4.

- **A robustly networked force improves information sharing**
- **Information sharing and collaboration enhances the quality of information and shared situational awareness**
- **Shared situational awareness enables collaboration and self synchronization, and enhances sustainability and speed of command**

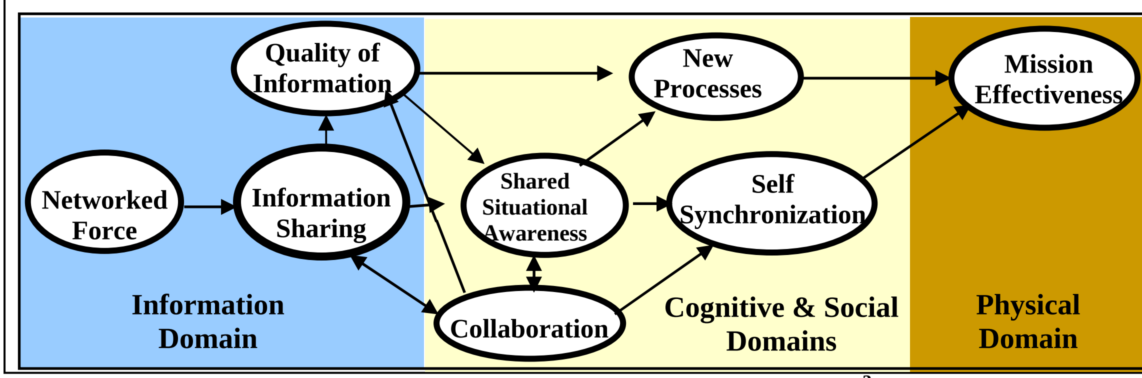

Figure 4: Tenets of Network-Centric Warfare[3]

The NCOW tenets from Figure 4 organize naturally into three clusters: (1) Get Connected, (2) Expose Data, and (3) Generate Knowledge, discussed below; when fully realized, they will promote greater information sharing across the Enterprise.

Get Connected

“Get Connected” includes understanding *who* and *what* (people and machine agents) are reachable *where* and *when*, and has as its basis information management systems that facilitate understanding. The major challenges in a network-centric environment center on moving from just physical asset management to parallel management of physical and virtual

[3] Modified from Alberts, Garstka, & Stein (1999).

assets such as services. Leading-edge research on this layer includes such areas as dynamic asset acquisition, deployment & configuration (and their implications for complexity), digital security, dynamic fault tolerance and performance optimization, as well as the formal analysis of human/system interactions during the generation, management and exploitation of information.

Expose Data

The primary focus of this volume is on the "Expose Data" and "Generate Knowledge" clusters. "Expose Data" addresses the challenge of ensuring that any consumer of data and information can discover and access/receive it from any producer in the Enterprise. Given the number, autonomy, and complex interactions of these groups, as well as the need to perform these functions rapidly in a dynamic environment, this is a daunting challenge that requires, at a minimum, a smooth transfer of information through machine-to-machine, machine-to-people, and people-to-people transactions. At its most mature level it reflects an intelligent capability to recognize and communicate information patterns across systems and to enable users to discover and retrieve key information -- even if they don't know it exists or how to request it.

Generate Knowledge

"Generate Knowledge" addresses the preparation of data and information for exploitation by human decision makers, and includes as its primary focus the fusion and aggregation of data and information for sense-making and situational awareness, as well as the cognitive and collaborative processes necessary to leverage this information for effective decision making in complex environments. From the perspective of our paradigm, warfighters and their missions are the "forcing function" for the development of technology and collaborative processes that provide "strong" support for decision-making in time-sensitive environments. This view is especially receptive to the increasing trend toward decision making at lower echelons, for scenarios, such as: (1) embedding close air support controllers with the forces they are supporting - while expecting them to remain tightly coordinated with other controllers, (2) enabling local medical assets to launch a coordinated response against multiple and dispersed biological attacks, and (3) supporting distributed operations - special operations forces and lower-echelon decision makers dealing with complex insurgencies.

Achieving Decision Superiority: The Canonical Enterprise Functions

At the beginning of this section, we introduced an overarching goal of the C2 Enterprise: "getting the *right information* to the *right people* at the *right time* to make the *right decisions*" (abbreviated as **R4**), and noted that this would be achieved through the integration of people, processes, and technologies performing the functions of generating, managing, and exploiting information more efficiently than our adversaries (or in rapid response to a natural disaster). This must be supported by a robust and adaptive information infrastructure (infostructure), whose availability under challenging and unpredictable circumstances is enhanced by characterizing and managing its sources of complexity.

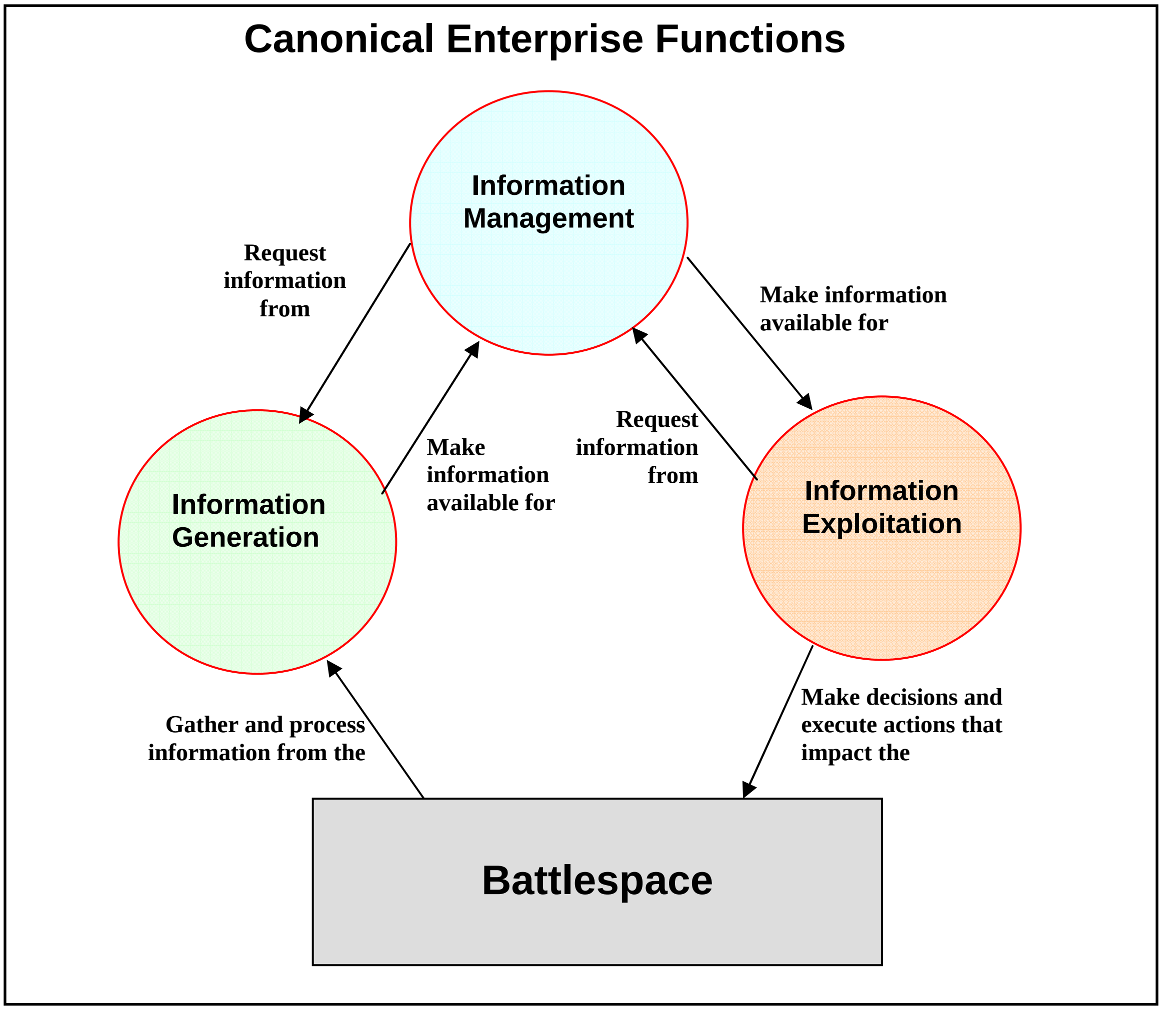

Figure 5: Interactions among the canonical enterprise functions and the battlespace

Figure 5 illustrates the interactions among these canonical functions. In NCOW terms, the battlespace comprises the "physical domain"; information generation and exploitation comprise an overlap of the "cognitive" and "information" domains, whereas information management resides in the "information domain" (Alberts, Garstka, & Stein, 1999). For the research and development of enterprise capabilities, this is helpful as guidance in determining what combinations of technologies need to be integrated to produce the target functionality. Within this context, the Infostructure can be viewed as an overlap between the cognitive and information domains. Ensuring its availability to warfighters or responders in unpredictable, emergent situations is critical to the achievement of R4.

Figure 6 shows the canonical functions in the context of the enterprise pattern they must fluidly form to support R4. The vertical axis (hierarchy) identifies information exploitation (people taking actions in C2) as the forcing function, with the generation and management of information providing strong support.

First order information flow suggests that information must be generated and managed before it can be exploited. However, different orders and configurations are possible with fully agile functionality (e.g., the iterative aggregation of information and knowledge to support time-sensitive team decision making).

For today's environments, it is necessary to be able to configure these functions in a rapid, on-demand fashion that can leverage the full power of the Enterprise. We briefly describe each critical function area below. Sections 2 through 4 of this volume provide more in-depth treatment of these functions, enumerating operational goals and objectives, as well as engineering design tenets, principles, and research needs.

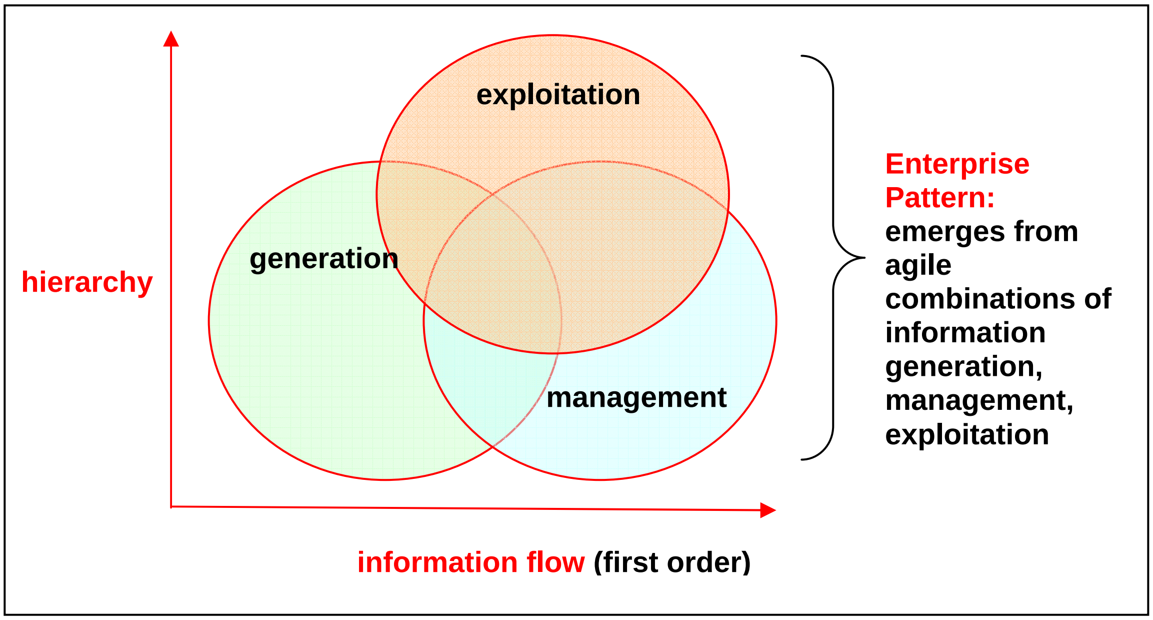

Figure 6: The canonical enterprise functions

Information Generation

Information generation is the aggregation and fusion of data and information from sensors and other sources in the C2 Enterprise for direct use by decision makers. As will be discussed in Section 2, information generation utilizes pattern recognition and information fusion technologies, can be fully or partially automated, and focuses directly on contributions to sense-making, situational awareness, and other decision making activities. An information generation function would heavily leverage the output of netted-sensors and any non-standard sources of data for better and timely sense-making on objects of interest (and their behaviors).

Information Management

To be meaningful, the products of the information generation function must be made available on the enterprise, and either "pulled by" or "pushed to" operators, often rapidly, to aid in their decision making. This requires an information management function of commensurate agility to help users discover the relevant information sources for aggregation, or, conversely, help discover users who, based on their activity and information request patterns, would benefit from data and information being generated elsewhere in the enterprise (often without knowledge of its existence). This management function is based in dynamic discovery, intelligent agents, and distributed computing technologies (among others), and requires an infostructure that is able to adapt to complexity at different levels and scales of the Enterprise

In our paradigm, Information Generation and Management provide strong functional support to the Exploitation of this information by people engaged in Command and Control.

Information Exploitation

Information exploitation refers to the direct use (explicit or transparent) by people of these functions and underlying technologies as well as the appropriate collaborative processes to make decisions. The Exploitation function is based in Cognitive Science and Collaborative Information technologies, and pays strict attention to how people best function under complex decision making situations, and how technology and processes can best be integrated to support them. The net effect of this paradigm, or agile combination of functions, is to add a new forcing function, people, to co-evolve with the existing forcing function, technology, to enable them to be more creative and innovative in taking actions in Command and Control. If this is done effectively, it will enable people to better leverage the power of technology and processes, rather than forcing them to compensate for their limitations.

As shown in Figure 7, the enterprise pattern comprised of the integration of these functions spans the major process nodes of network-centric information flow in a comprehensive way. Thus, researching and developing capability in the integration of these functions has the potential to yield significant returns-on-investment for decision support and its dependence on the underlying infostructure (i.e., its availability).

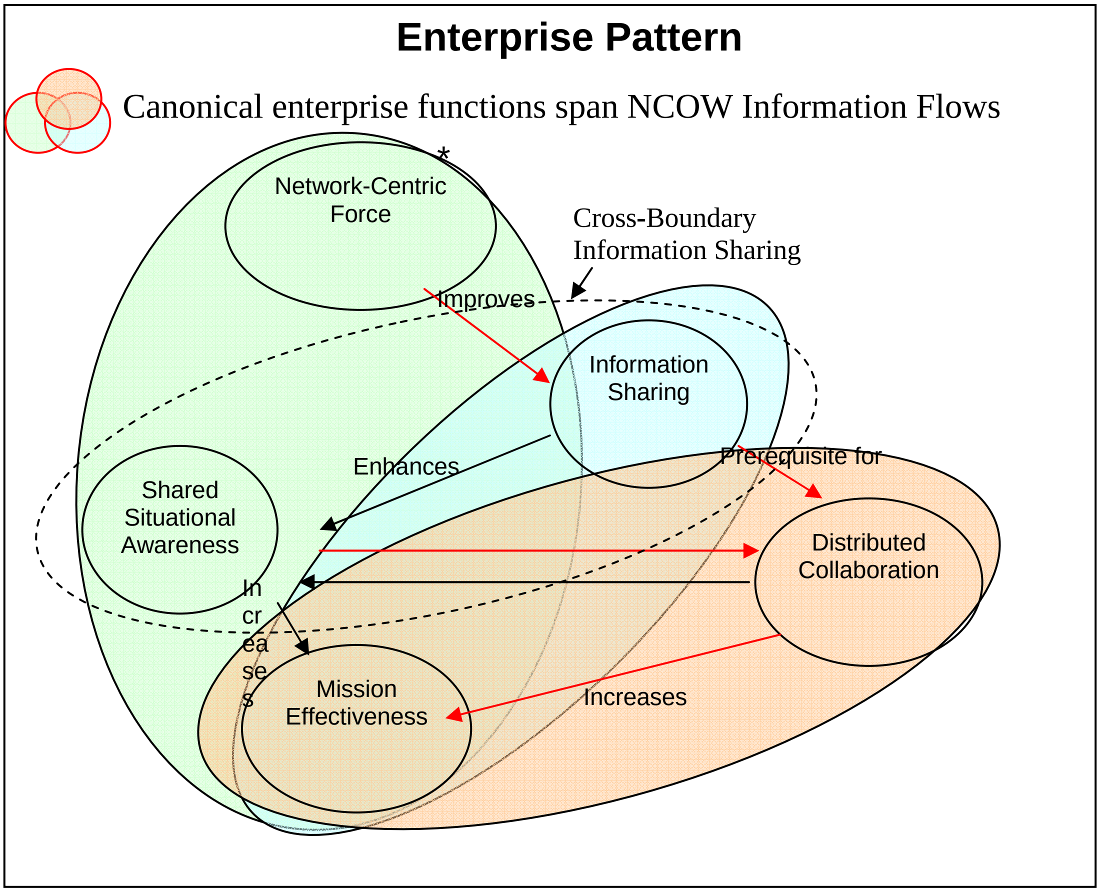

Figure 7: How our enterprise research paradigm spans the nodes of network-centric information flow[4]

For a closer look at this, Figure 8 shows a hierarchical technology pyramid that underpins our paradigm and much of enterprise technology development and application. A facile mapping to this pyramid would place exploitation in the decision support layer, generation in the boundary between the decision support and information technology layers; management, especially when infostructure complexity is considered, firmly connects the information technology and network layers of the pyramid. All of this is highly dependent on strong foundational support (sensors and enabling technologies).

---

[4] Modified from Mitchell, Cummings, & Sheridan (2004).

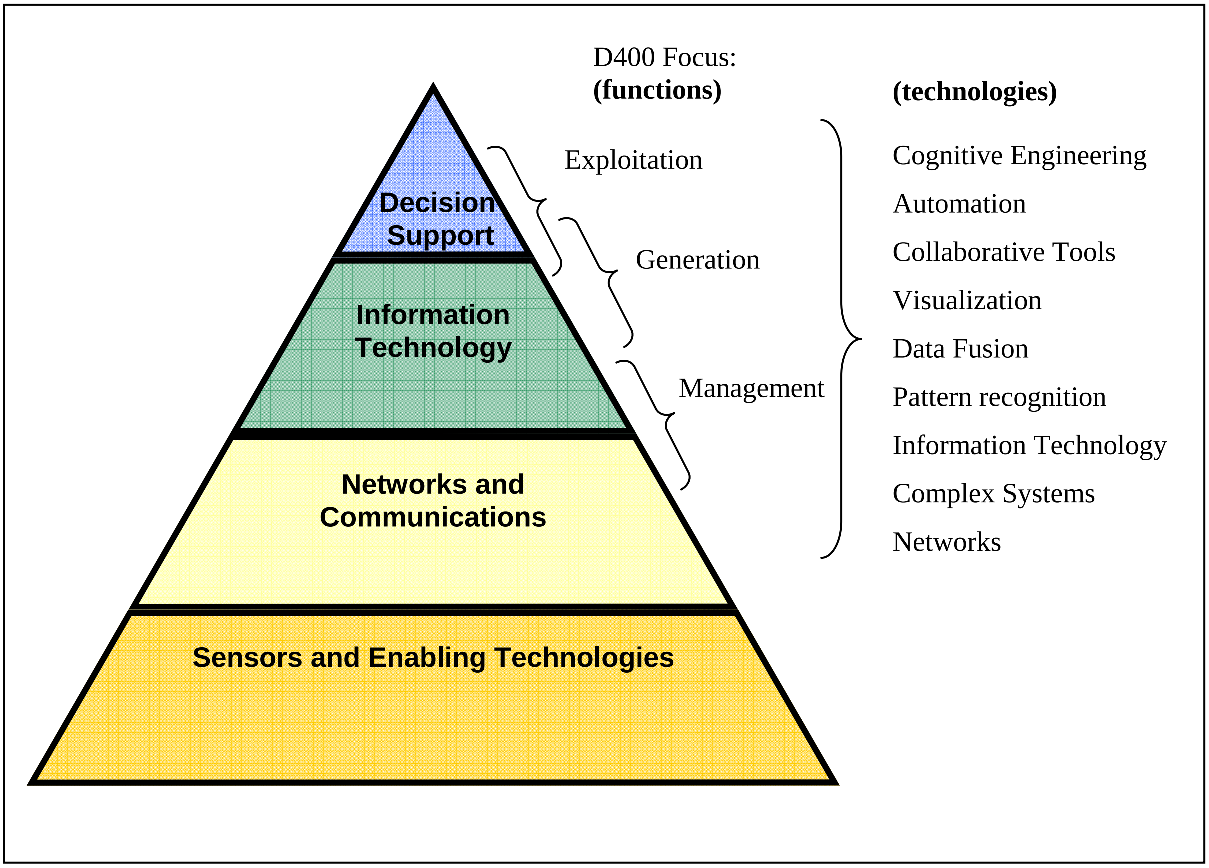

Figure 8: Enterprise technology layers

Summary: The Remainder of this Volume

In this section we have briefly discussed the complex challenges the military will face in future warfighting scenarios – from both conventional and asymmetrical threats. We have identified the response to these challenges as the transformation of the military into a network-centric enterprise, within which agile information generation, management, and exploitation, fed by netted, heterogeneous sensors, and supported by a robust infostructure, are necessary conditions for the type and magnitude of the information and decision advantages required. It should be pointed out that the scope of the research landscape associated with this functionality is very large – as is the landscape of the operational and engineering practice venues it targets. The research paradigm introduced here, and treated in more detail in subsequent sections, covers at best a small, but potentially important part of this landscape, based in the integration of Complex Adaptive Systems, Cognitive Science, Information Technology, and Enterprise Systems Engineering.

2 Agile Information Generation (The Right Information)

Introduction

A Definition

What is information generation? Consider the following as one possible definition:

*"Information generation is a process which involves the collecting, processing and displaying of data (i.e., facts of various kinds, informed opinions, wild guesses, etc.) from which one can answer certain relevant questions (**who, what, where, when, why**) relevant to a given situation. This process may also involve the allocation of resources to gather more data in the event that any one or more questions cannot be answered satisfactorily."*

Other equally descriptive definitions are certainly possible, but in the broadest sense, information generation is a process which contributes to or enables the understanding of a dynamic situation. Of course, the degree to which such understanding is needed depends greatly on the problem to be solved (i.e., the context). For example, it may be sufficient to know where an object (e.g., a person, a vehicle) is located, but not care about its relationship (if any) with other objects. Furthermore, generating information in an ***agile*** manner considers both the need to be ***adaptable*** (i.e., modifying a process to accommodate changing circumstances) and ***flexible*** (i.e., modifying a process to accommodate changing requirements or goals) in one's process.

In the discussions that follow, we will consider "data" to be the input to a first level of an information generation process, and "generated information" to be the output. This "generated information," in turn, may serve as the input to a second, third, etc. level of an information generation process. Also, we will sometimes refer to "data" and "generated information" collectively as "elements."

Models for Information Generation

One model for the information generation process, as it applies to a fairly broad class of problem, the data fusion problem, is the ***Joint Directors of Laboratories (JDL) Data Fusion Model***. Informally speaking, data fusion is a process that combines information from multiple sensors and related information sources to achieve better inferences than could otherwise be achieved with just a single sensor or source. This model, originally developed with military systems in mind (but later extended to commercial systems), is a conceptual model which seeks to identify basic processes and functions which may be required to implement a data fusion system. It defines a basic process flow and identifies processes and representative functions. Rather than being a "blueprint" for the development of a data fusion system, the Model is intended to be generic and serve as a basis for common understanding and discussion.

Figure 9 below represents a revised version of the JDL Data Fusion Model. Note that the Model is comprised of five levels of data fusion processing and the interaction with sources (of data), a database management system, and a human/computer interface.

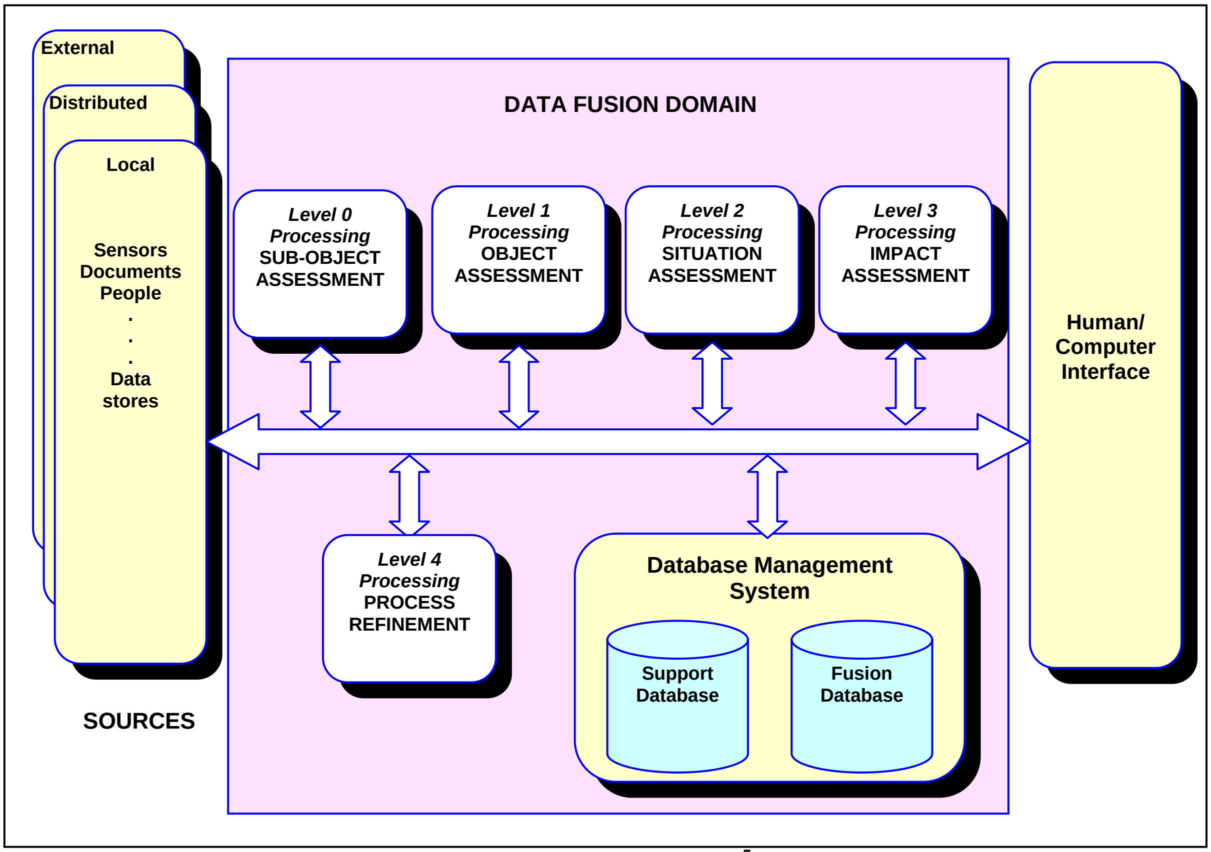

Figure 9: The JDL Data Fusion Model[5] (Revised 1998)

Descriptions of each level (provided as part of the model) are provided below.

- Level 0 – Sub-Object Data Assessment: Estimation and prediction of signal- or object-observable states on the basis of pixel/signal level data association and characterization.

- Level 1 – Object Assessment: Estimation and prediction of entity states on the basis of inferences from observations.

- Level 2 – Situation Assessment: Estimation and prediction of entity states on the basis of inferred relations among entities.

[5] From Hall & Llinus (2001).

- Level 3 – Impact Assessment: Estimation and prediction of effects on situations of planned or estimated/predicted actions by the participants (e.g. assessing susceptibilities and vulnerabilities to estimated/predicted threat actions given one's own planned actions).
- Level 4 – Process Refinement (an element of Resource Management): Adaptive data acquisition and processing to support mission objectives.

The concept of situational awareness plays a large role in the processes concerned with cognition, decision-making and collaboration in military as well as non-military domains. As defined by Endsley (2000), situational awareness is simply "knowing what's going on around you." Domains in which situational awareness is studied include aircraft piloting, education, driving, train dispatching, machine and systems maintenance, weather forecasting, and others (Endsley, 2000). Furthermore, Endsley (2000) proposes a ***model for situational awareness*** comprised of three levels:

- Level 1 – Perception: "The perception of cues" in an environment.
- Level 2 – Comprehension: "How people combine, interpret, store and retain information…it includes the integration of multiple pieces of information and a determination of their relevance to the person's goals."
- Level 3 – Projection: The "ability to project from current events and dynamics to anticipate future events (and their implications) allows for timely decision-making."

Note the similarity between these two models. For example, the "situation assessment" level in the JDL model (i.e., Level 2) describes a process in which one attempts to establish relationships among objects, once located and, perhaps, identified. In Endsley's model, the "comprehension" level (i.e., Level 2) deals with the integration of perceived cues (akin to "objects") and determination of the relevance of these cues against one's own goals. At this level, both models are concerned with going beyond the individual "collected bits" – they are concerned with making sense of the aggregation of information at a higher level.

Considerations for an Agile Information Generation Process

Information generation is more than just implementation of algorithms to affect, for example, the various levels of the JDL Data Fusion Model. "Number crunching" by itself can't hope to bring sufficient understanding that will allow one to answer the questions: who, what, where, when, and why? It is one thing to generate information; it is another to make sense of it (***cognition, see Section 4***), act upon it in an appropriate and timely manner (***decision-making, see Section 4***), and to share data and information with others for their own mutual benefit (***collaboration, see Sections 3 and 4***). The last observation is an important one. Even within the context of the JDL Model (which has a highly-automated flavor), the interactions among the human elements of a system are vital to the success of the information generation process – in terms of putting information in the proper context, resolving ambiguities, and sharing this information in an appropriate manner.

The Information Generation Environment

Increased Availability of Data

Consider a notional (and scaled-down) information generation environment as depicted in Figure 10. Here we see local clusters of information nodes. The "local-ness" of a cluster relative to another may be attributed to, for example, physical proximity or the likelihood of affecting some form of interoperability between them. Within each cluster there is some number of nodes with a certain degree of connectedness. Each node has the potential to be a producer as well as a consumer of information. While the number of clusters and nodes within each cluster is small in this representation, in reality, theses numbers could be a good deal larger.

Each node has its own needs for information, which may be satisfied based on its own data sources, or in combination with data from other nodes within and outside of its own cluster. Furthermore, it is expected that these information nodes will act in a manner to achieve some mix of well-defined and open-ended goals. To this end, information nodes will engage each other in a collaborative way, sharing data sources, information (at various levels) and information "needs" and "goals" throughout the duration of their "interaction" (which could, in principle, be "forever").

Finally, it may very well be the case that any node (or cluster of nodes) will be unaware of, at any given point in time, the existence and, therefore, the potential value of other information nodes. (The single node in the dashed box in Figure 10 is meant to represent a node whose existence is yet unknown to the two local information node clusters.)

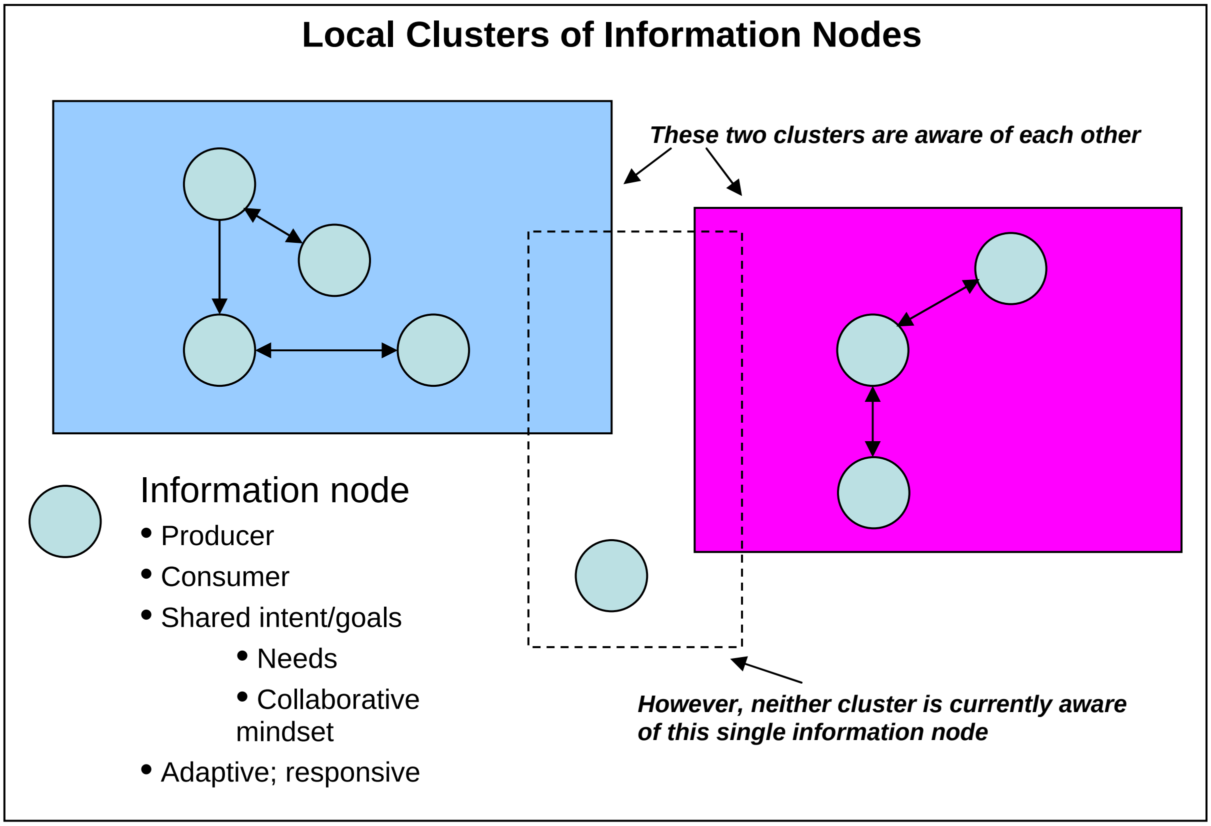

Figure 10: Notion of an enterprise from an information node point-of-view

Availability of "New" Data Sources

Sensors that exploit various parts of the electromagnetic spectrum (e.g., radar, electro-optic, etc.) constitute important sources of data in a many types of military enterprises. In particular, the data that allows for the generation of target attributes such as location, kinematics, and identification almost always originates with such sources. These target attributes are, to be sure, important dimensions of situational awareness (and in some instances, they're all that matters). However, the increased use of internet chat, instant messaging technologies (particularly, in military operations), as well as email and web logs (blogs) have made possible another dimension of situational awareness: team awareness. Awareness of the changing roles, responsibilities and knowledge of people (i.e., members of a team) participating in an enterprise can be discerned by exploiting information generated by these "non-traditional" data sources.

Greater Need for Sharing Data at All Levels

Requirements for the effectiveness of any decision-making process within an enterprise are, generally, derived from operational needs. In recent years, the need to reduce fratricide has lead to the development of Blue Force Tracking (BFT) technologies providing high levels of situational awareness. Here, the requirement demanded a more comprehensive and dynamic situational awareness that was achieved, in part, by the availability of multiple sources of data and information.

In other decision-making processes, the increased accuracy and timeliness of a reported object attribute (e.g., the location of a high-value target) may be of primary importance. As with the BFT problem, there is a need to share data to achieve required accuracy and timeliness.

Information "Needs" and "Goals" Not Always Known in Advance

It may very well be the case that for all information nodes within an enterprise, their information "needs" and "goals" will always be known, well-defined and well-articulated. For example, ground moving target indicator (GMTI) platforms may have associated a priori data collection plans from which operators may base their operation of the on-board sensor (collection) assets. In this case, information needs are known and can be mapped into specific resource management actions. Subsequent collection will fulfill the information needs. Beyond the immediate needs embodied in such a collection plan, a node may also possess information "goals," motivated by an open-ended or, perhaps, ill-defined problem.

Whether presented as a well-defined need or an open-ended goal, it is assumed that information will be generated based on data that is available at a local node or at other already-connected and participating nodes. Such an assumption may impose a limitation on the information generation process: information nodes which exist, but are yet unknown, will not be able to contribute their data to the process. That is, enterprise nodes will not take advantage of the opportunities afforded by the data available at other nodes.

Greater Potential to Task Data Sources to Gather What's Needed

In the future, individual sensor platforms (e.g., Multi-Sensor Command and Control Aircraft (MC2A)) will be capable of (improved) tasking of not only their on-board sensor assets, but also those of off-board sensors. Far from being a case of "selective interoperability," these platforms will be elements of larger sensor networks, each working in a collaborative fashion to achieve information needs and goals. Some primary examples of these networks include the Single Integrated Air Picture (SIAP), Network-Centric Collaborative Targeting (NCCT), and the Command and Control (C^2) Constellation.

Data Sources "Experience" the Complexity of an Environment

As discussed in the overview of this volume (Section 1), "emergence," as an element of complexity, may occur within and affect elements of an enterprise in a number of ways. In the case of adversary-created emergence, changes in enemy tactics serve to adapt or interact with our efforts to achieve military goals. To the extent that data sources (e.g., sensors, human intelligence, etc.) are able to "observe" these dynamics within the environment, people and processes within the enterprise will need to understand (at possibly many levels) the implication(s) of this emergent behavior.

Data with Future Value

Information has its greatest value in a current context. Arguably, information that is only relevant to a particular situation may lose its value at the end of that situation. However, this does not necessarily mean that the data is without value in the future. The ability to store or "warehouse" data or generated information may add value to an enterprise in the long run, if one considers retrospective or "forensic" analyses.

Information Generation Challenges

Correlating Data from Diverse Sources

With the increasing availability of data from information nodes, particularly those nodes as yet unknown to other local clusters of nodes, comes the challenge of associating (or "correlating," the terms are used interchangeably, here) the data or information from two or more nodes (or even within a single node). In addition, association processes may be carried out over time.

In the data fusion problem, one seeks, for example, to establish whether an observation (e.g., a geo-location on an object) from more than one sensor can reasonably be attributed to the same object - that is, one seeks to correlate the two observations. In doing this, it is then possible to "fuse" the two observations to obtain a more accurate geo-location. In other settings, the association of data or information may be, for the most part, an end unto itself. For example, the association of intelligence reports from different sources may be all that is required for understanding.

In general, the information generation process is likely to require, at various stages, the association/correlation of data or information. Currently, systems are designed with specific requirements for the types of association/correlation to be carried out. For example, the multi-source integration application in the Airborne Warning and Control System (AWACS) platform is designed to correlate observations from its on-board sensors (e.g., radar and identification friend or foe (IFF)) with observations from off-board sources via the Link-16 tactical data link. Here, the "character" of the observations is well-defined and known a priori (i.e., you known the structure of the data), and the algorithms which affect the association are (for the most part) specially "tuned" to this character. In doing this, one ensures effective (accurate and timely) association in an environment where the particulars of information exchange have been established.

In the broader enterprise, however, the potential exists to interact with information nodes that generate data or information which could be of current or future value to another node. While one does not expect an enterprise to encompass an infinite variety of data or information sources, one can reasonably expect to find some source whose “character” (i.e., data structure or schema) is not known to you a priori but may be useful in the future. The problem is not so much that the data’s character is not known (because it can be “discovered” by its publication), but rather it is the ability of a node to effectively associate/correlate this new data source with existing data sources once the data’s structure is known.

Managing Information “Needs” and “Goals”

Most often, information nodes, as producers of information, work against a collection of well-defined information “needs.” Here, the problem is known and understood in terms of what information is required to affect a decision or to attain some degree of understanding. However, when a problem is presented in an open-ended way, it may be the case that not all information needs can be articulated. Rather than specific “needs,” broad information “goals” may be established.

In an enterprise environment, the availability of data or information from yet unknown information nodes represents both a challenge and an opportunity in terms of developing and refining both information “needs” and “goals.” The following assertions (excerpted from (Alberts, Garstka, & Stein, 1999)) on the value-creation potential of networks, help shape a view of Network-Centric Operations and Warfare (NCOW) in terms of both challenges and opportunities:

> “Thus, establishing a direct relationship between information and value is at the heart of value creation in the Information Age and is fundamental to understanding the power of network-centric operations. In addition, we believe that:
>
> 1) most potential interactions will never take place;
>
> 2) the value of interactions will differ significantly;
>
> 3) there will be islands of dense and intense interactions that will dominate the value function;
>
> 4) the value of a given interaction will be a function of the content, quality, and timeliness of the interaction; and
>
> 5) N-way interactions will be the most significant in value creation.”

The obvious challenge implied by such a view is to determine which interactions will be of the greatest value, from the perspective of all network nodes. However, value need not be restricted to that which contributes to reducing uncertainty in one’s present awareness or understanding; <u>value can also found in that which reduces future uncertainty</u>. In this sense, an enterprise has value in the form of both present and future opportunity.

Lastly, the network-centric view does not directly address the dynamic nature of the network: the necessity or desire to “adapt” in response to changes in the battlespace environment.

Exploiting Elements of Complexity within an Environment

In the emerging concept of NCOW, understanding the behavior and relationships among objects within an environment becomes the focus more so than the understanding of individual objects (Moffat, 2003) In such an enterprise, for example, one concerned with NCOW, elements of complexity, such as self-organization (emergence) and adaptation, can arise. One example is the clustering (i.e., self-organization) of various types of tactical units in a land warfare environment. This clustering (which is part behavior, part relationship) may be observed (most commonly, by sensors) and data produced as a result of these observations. That is, **there will be complexity in the data itself** because it mirrors a complex system. Thus, certain elements of complexity will be present in the situational awareness of this land warfare environment. However, these elements may not always be readily recognizable. To the extent that such self-organization (here, among tactical land units) is recognizable and results in improved situational awareness, new behaviors may emerge among other objects within the environment, say, from the opposing tactical forces. Here, improved situational awareness produces emergent behaviors within the environment.

In this NCOW enterprise, objects are not restricted to just those active participants (e.g., objects on the battle field), but also those participants who may be observing the environment and making certain decisions as to future courses of action. These decision-makers themselves may "engineer" their own complexity. For example, self-organization (emergence) may be engineered through the collaborative process in which decision-makers share data, information, and information "goals" and "needs." That is, **there will be complexity within the collaborative decision-making environment**. Here, the medium for collaboration may be as simple as verbal communication or it may be of a more "complicated" form such as internet chat or instant messaging. Regardless of the medium, collaboration can bring about emergent behavior, often driven by the "forces" of social cohesion and embeddedness (Moody & White, 2001). In such cases, self-organization may directly affect "team awareness;" that is, an understanding of what others do and know, and what role they have in the larger team. One can assert that improvements in team awareness lead to improvements in situational awareness.

Information Generation Tenets and Design Principles

Make Explicit the "Quality" of Data or Generated Information at All Levels

In almost every situation and at almost every level, to effectively use data or generated information as input to a decision-making process, the "quality" of these elements must be known. Consider a multi-dimensional view of "quality":

- **The pedigree (origin) of data or generated information –** This can most readily be achieved through the use of standardized "tags" and nomenclature. For example, the origin of information can indicated using a digraph/trigraph approach (e.g., AB, DEF, etc.). In instances where new information is being generated, the origin of the constituent elements can be retained.

- **The accuracy of, or uncertainty in, data or generated information –** In general, for continuous information states, accuracy, or uncertainty, can be expressed as a probability density function (PDF) of the error in the information state. Often, however, accuracy is expressed by only the first two moments of the error PDF (e.g., a two-dimensional "error ellipse" representing the bias and "scatter" of an estimated information state). In the case of discrete information states, the probability distribution over all possible outcomes of the information state can be used to represent uncertainty. For example, in the case of the identification of an object or an event, the probability of a correct identification can be provided. Of course, assessment of the accuracy of information generated by people (e.g., through observation and analysis, reasoning, or opinion-making) is a much messier endeavor.

- **The latency associated with data or generated information –** Latency is loosely defined as the difference between the time at which information was generated and the time at which the data comprising the information was produced. For example, an intelligence report was made available two minutes after the creation of the constituent intelligence contact. If latency is random rather than deterministic, a statistic (e.g., a 90^{th} percentile value) should be made available with the information.

- **The "freshness" of data or generated information –** One can represent the degree of "freshness" in information simply by keeping track of the time since the information was (initially) generated or last updated. From an information producer's point of view, this merely requires placing a "time stamp" on data.

Develop, Publish and Manage Information "Needs" and "Goals"

Development of information "needs" and "goals" is a necessary and prudent first step to effective information generation. It places bounds on information from the point-of-view of both the producer and the consumer. Publication of needs and goals is a powerful idea; it allows for the possibility of one information node to leverage information available at another node. Finally, management of information needs and goals should be considered not just in light of having achieved certain organizational goals (e.g., the successful prosecution of a time-critical target), but also by taking into account the future (projected) value of data.

Underlying this "develop, publish, and manage cycle" is the ability to express, or represent, information goals and needs. Consider three broad approaches:

- **Specific statement of need –** The statement "I require position and kinematic data on track number ABCD" is explicit and unambiguous. Here, the consumer is providing a specific request for information, thereby strictly limiting the amount of information a potential producer would need to disseminate. Providing a quality metric for position and kinematic accuracy may further limit the amount of disseminated information.

- **General statement of need** – The statement “I require any data relating to ground moving objects between latitudes X and Y and longitudes W and Z” is still explicit, but is now somewhat ambiguous. A potential producer of information would need to decide, based on available bandwidth, just how much information on how many objects could be disseminated. Here, the consumer is “hedging” against unknown and, possibly, future information needs by being less specific.

  This particular general statement of need can be refined somewhat by ascribing a relative value to classes of ground moving objects. For example, transport erectile launchers (TELs) may be “high” value, tanks may be “medium” value, and personnel carriers may be “low” value.

- **Hierarchy of goals –** Information needs, whether specific or general in nature, are often derived from goals established within an enterprise for a particular mission. So, rather than publishing needs, one can publish a set of goals, which allows an information producer to decide how to best satisfy what they understand to be the needs of a potential information consumer. For example, goal lattices have been used to represent a hierarchy of goals, including a relative apportionment of value among (possibly competing) goals (McIntyre, 1998).

Associate/Correlate Data and Generated Information

Association/correlation, either as a first step to “fusing” data or generated information, or as an end unto itself, is at the center of an information generation process which deals with multiple information sources. Association/correlation should be carried out with the following in mind:

- **Alignment to a common spatial and temporal frame of reference –** This is the first step in any association/correlation process. In the spatial dimension, a transformation of basis vectors from one coordinate system to another is required to affect this alignment. In the case where the spatial data is textual and not numeric, alignment constitutes translation to a common basis language. In the temporal dimension, interpolation or extrapolation to a common time is required.

- **Remove or otherwise account for bias in the constituent data or generated information –** Here, bias is meant as that part of the measurement of an object’s attribute (e.g., geo-location) that has a constant offset from the true value of the object attribute, which cannot be eliminated by repeated measurement. For example, measurements made by a radar sensor contain an azimuth bias when a misalignment is present between a measurement axis and a reference axis (e.g., the direction of truth north).

- **Utilize the accuracy of the data** – When possible, use the accuracy of the data to assess the degree of similarity between objects. Using the known uncertainty that comes along with a measured value of an object attribute (e.g., a geo-location) will allow for a better "quality" of association/correlation.

- **Allow for the possibility of object attributes at different scales of measurement** – Not all object attributes have values on a numerical (interval or ratio) scale (e.g., value = 1.234). Some attributes will have values on a nominal (e.g., value = yes or no) or an ordinal (e.g., value = 2, which is greater than 1 but less than 3) scale. The association/correlation process should not disregard or under-utilize attributes on these "non-standard" scales.

- **Allow for the association/correlation of objects over time –** Depending on the threshold(s) used, more than one "epoch" may be required to obtain a sufficient "quality" of association/correlation. The usual trade-off will be time vs. quality of the result.

Enable the Fusing of Data or Generated Information

While not always necessary to attain a desired level of understanding, the "fusing" of data or generated information requires that certain conditions be met before constituent elements (i.e., data or generated information) are combined:

- **Utilize and then reassess the "quality" of data or generated information** – The fusion process should use the known quality of the constituent elements and should determine the quality of these combined elements once fusion takes place (see discussion above).

- **Alignment to a common spatial and temporal frame of reference –** See discussion above.

- **Remove or otherwise account for bias in the constituent elements –** See discussion above.

- **Retain links to constituent elements** – Links to the constituent data or generated information are retained as part of the result. At a minimum, the pedigree (origin) of each of the constituents should be retained.

Use Visualization to Understand Relationships in Data or Generated Information

Where information is in the form of a relationship (e.g., making the statement that one object is somehow "related" to another object), visual representations may be the most expedient and reliable means of highlighting such relationships. Often, visualization involves the textual representation of data (e.g., data available in tabular form and across multiple tables).

Other visualization approaches involve the construction of a hierarchy (or "tree") of data or of generated information. Examples of the use of visualization in the "detection" of relationships in data include the clustering of air traffic control flows and the construction of drug traffic network diagrams (DeArmon, 2000).

Enable the Recognition of Complexity in Data and Decision-Making Environments

Recognizing complexity (e.g., self-organization, adaptation) within an enterprise (which includes the data, the decision-makers, and the enterprise itself) requires a combination of human and machine processing as well as their interaction. Regardless of whether an element of complexity is "engineered" or "naturally-occurring," its recognition will depend on the specific model applied to the Complex Adaptive System (CAS) under consideration. There are a number of ways to model a CAS, with each approach grounded in a particular discipline (Ahmed, Elgazzar, & Hegazi, 2005). There are, however, some general "principles" to keep in mind, which may allow one to, at least, initially capture certain elements of complexity:

- **Aggregate data or generated information –** Clustering of multi-dimensional objects may, at least partially, reveal emergent properties of an enterprise. Here, the less-algorithmic approaches to clustering, such as visualization, should be considered. And, as with association/correlation, object attributes on different scales should be considered.
- **Assess relationships –** To the extent that the selected form of clustering does not adequately capture a relationship, other approaches (which may pick up where clustering left off) should be considered. Again, visualization may get you further than purely-algorithmic approaches.
- **Monitor for change –** The time-series behavior of objects (or aggregations of objects) should be examined periodically to "detect" and characterize underlying dynamics.
- **Allow for "push" and "pull" interactions between human and machine –** Often, more meaningful aggregations and relationships can be obtained when a human "seeds" the process used by the machine. This is one type of "pull" interaction.

Warehouse Data or Generated Information at All Levels

The "warehousing" of data or generated information from a current context (e.g., a military engagement) will enable their ready analysis in the future. Such retrospective or "forensic" analyses may facilitate the discovery and modeling of new information and relationships. Beyond the very real issues surrounding what to store and how to store it, other considerations include how to deal with “derived” data types, such as a network or a pattern expressed as a time series, or perhaps a set of clusters.

Apply Meaningful “Tags” to Data or Generated Information

Data or generated information should be “tagged” appropriately to facilitate future retrieval and processing. Ideally, the tags should be derived from a vocabulary of terms developed for a specific domain. Here, one can look to the established registries containing such vocabularies. For example, vocabularies and grammars relating to the Department of Defense (DoD) can be found at the DoD XML Gallery, http://diides.ncr.disa.mil/xmlreg/user/index.cfm).

By way of summary, Table 1 “maps” tenets and design principles to the information generation challenges they address. As one might expect, some tenets, for example, applying meaningful “tags” to data, address all challenges to information generation within an enterprise. In this case, such “tagging” allows data and generated information to be readily understood by both human and automation within an enterprise.

	Challenges		
Tenets and Design Principles	Correlate Data from Diverse Sources	Manage Information Goals	Exploit Complexity
Make Data "Quality" Explicit	☑		
Develop, Publish and Manage Information Goals		☑	☑
Associate/Correlate Data	☑	☑	☑
"Fuse" Data	☑		☑
Use Visualization to Assess Relationships	☑		☑
Enable Recognition of Complexity		☑	☑
Warehouse Data			☑
Apply Meaningful "Tags" to Data	☑	☑	☑

Table 1: Information generation challenges and tenets/design principles

Enabling Technologies for Information Generation

There are a number of technologies that enable various aspects of agile information generation within an enterprise. Below is a listing of some of these major technologies and disciplines:

- Data fusion
- Pattern recognition (in particular, data mining)
- Visualization
- Text and information extraction
- Complexity theory
- Intelligent agents
- Operations research
- Evolutionary and genetic algorithms
- Simulation
- Metadata, schemas and ontologies

- Data warehouses

Disciplines such as operations research and simulation are well-established with wide application and representation in the technical literature. Others technologies, like evolutionary and genetic algorithms, and intelligent agents, are just “coming into their own,” relatively speaking. Complexity theory represents somewhat of a hybrid discipline, blending new concepts and technologies, such as the use of agent-based modeling to analyze self-organization and emergence, with “traditional” technologies such as networks. We briefly discuss two of the most important enabling technologies for agile information generation: data fusion and data mining.

Data Fusion

The JDL Data Fusion Model, as described earlier, not only provides a framework for discussing the elements of data fusion processing, but also hierarchies of functions and associated enabling technologies (techniques). What follows are some examples of technologies and disciplines used to enable the processing associated with JDL Model Levels 1 through 4, particularly as they relate to the development of data fusion systems for military application (Berube, 2002).

Level 1, Object Assessment, is concerned with the localization and identification of objects. One function within this level of processing deals with estimating the position, kinematics (i.e., dynamics) and other attributes of an object, which is a critical function of almost all military data fusion systems. Figure 11 presents a hierarchy of techniques associated with this function. Here, we see that techniques from disciplines such as operations research, evolutionary and genetic algorithms, digital filtering and stochastic estimation are prominent in their application. In particular, the application of the sequential Kalman filter (both in its linear and non-linear forms) is nearly ubiquitous in military data fusion systems.

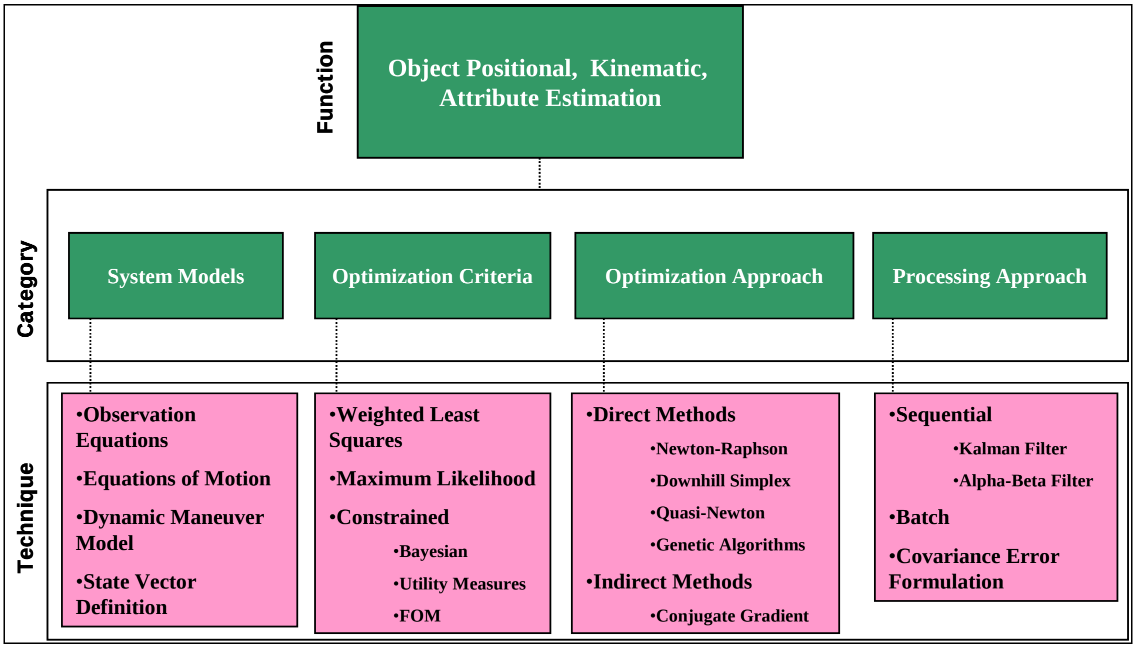

Figure 11: A hierarchy of techniques associated with estimating object attributes

Level 2, Situation Assessment, involves the dynamic generation of a description of current relationships among objects and events in the context of their environment. This processing typically involves aggregating objects, interpreting events and activities, and context-based reasoning. Technologies taken from the fields of artificial intelligence and pattern recognition dominate applications at this level. Examples of these technologies include rule-based and knowledge-based systems employing logical templates, case-based reasoning, fuzzy logic, and clustering.

Level 3, Impact Assessment, involves the projection of current situations into the future to draw inferences about enemy threats, friend and foe vulnerabilities, and opportunities for operations. This processing typically involves aggregate force estimation, intent prediction, multi-perspective analysis, and temporal projections. Technologies prevalent in Level 2 are also widely used in Level 3 applications.

Level 4, Process Refinement, involves monitoring the overall data fusion process to assess and improve real-time system performance. Here, processing functions include performance evaluation, process control, determining source requirements, and mission management. Important disciplines at this level include operations research, in particular, optimization and decision theory.

Data Mining

Data mining is the art and science of finding "meaningful" relationships and patterns in large amounts of information (Cabana & Swarz, 2000). Applications of data mining technology are numerous in both commercial and government domains. On the commercial side, data mining has been used for market basket analysis, credit risk assessment, fraud detection, and logistics/inventory modeling. On the government side, data mining has found application in Internal Revenue Service (IRS) tax compliance, aviation safety, and U.S. Customs Service counter-drug intervention (Cabana, Babich, & Washburn, n.d.).

Problems in data mining may be divided into two classes: predictive and descriptive. In predictive data mining problems, a mathematical model (or set of models) is developed that allows the user to predict a new outcome (or value) based on information about already known (i.e., historical) cases. This is perhaps the most familiar form of data mining and is more commonly referred to as "supervised classification" or "supervised learning." The technologies most commonly applied to this class of problem come from the disciplines of multivariate statistics and artificial intelligence, and include linear and logistic regression, discriminant analysis, neural networks, and decision trees.

In descriptive data mining problems, the goal is to segment information (cases) into some number of distinct groups, where objects in each group are more "similar" to each other than objects in other groups. This problem is more commonly referred to as "unsupervised classification" or "unsupervised learning." These problems require a definition of "similarity," which is usually dependent on the problem being studied. Often, the concept of "distance" between information (cases) is used as a measure of similarity. As with supervised classification problems, the technologies most commonly applied here come from the disciplines of multivariate statistics and artificial intelligence. One general category of technologies is that of data clustering. Figure 12 presents a very high-level "sketch" of clustering and its application to a data mining problem: determining segments of fighter squadrons with similar engine failure histories. In this very simple example there are three groups of fighter squadrons with similar histories, one of which contains two geographically widely-distributed squadrons. Among the technologies that may be applied to such a problem, K-means clustering is one or the more intuitive and easily-programmed of those listed in Figure 12.

- **Find groups of similar data items**
- **Simplest data mining technique to use/understand**
- **Requires some definition of "distance" (e.g. between travel profiles)**

Uses:

- **Demographic analysis**

Technologies:

- **K-means clustering**
- **Agglomerative clustering**
- **Self-Organizing Maps (Kohonen networks)**
- **Probability Densities**

"Groups of squadrons with similar engine failure histories"

- 510FS (Aviano)

- 117FW (ANG) (Atlantic City), 35FW (Kunsan)

- 62FS (Luke)

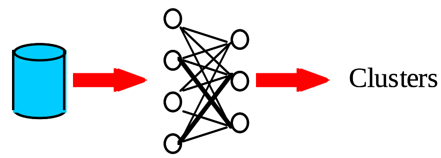

Figure 12: Clustering and a data mining application[6]

Information Generation Use Cases

There are a variety of research issues relating to the development of agile information generation capabilities in an enterprise. We list a few important issues below, grouped according to a specific "challenge" (see Table 1 above) to engineering an enterprise:

- Correlate data from diverse sources
  - Ability to correlate sources such as imagery, video, internet chat and instant messaging with structured sources
  - Ability to do "quick, good enough" correlation with any data type
- Manage information goals
  - Capabilities-based vs. requirements-based publication of information
  - Development of information goals based on "opportunities" derived from (emerging from) situational awareness
- Exploit complexity
  - Algorithmic and visualization-based approaches to analyzing elements of complexity (e.g., emergence)
  - Real-time data warehousing to support analysis of complexity

Below, we step through a series of example use cases in information generation research.

[6] From Cabana & Swarz (2000).

Correlating Data from Diverse Sources

As an example of correlating data from diverse sources, consider the problem of exploiting elements of internet chat and structured data (e.g., GMTI reports) in a time-critical targeting environment. In such environments, operators who rely heavily on chat as part their sense making processes have to manually (if they do so at all) establish relationships between chat and structured data, often under time pressure.

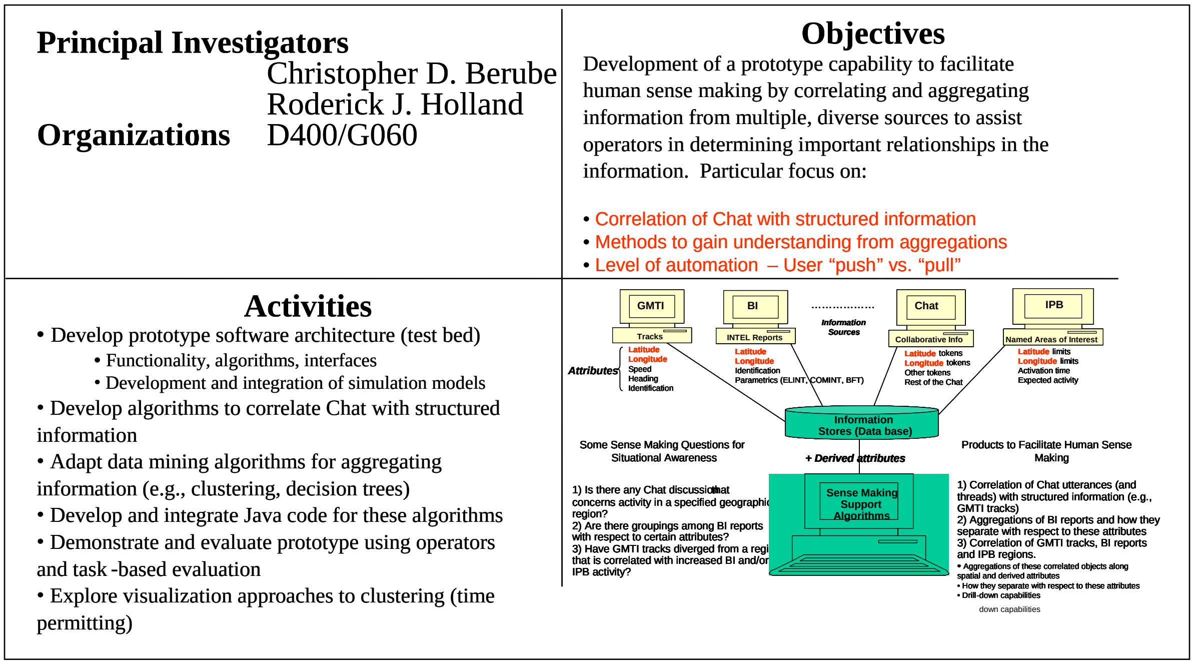

Figure 13: "Facilitating Sense Making for Situational Awareness"

To assist in establishing such relationships, an FY06 Air Force sponsored research project has been conducted. Figure 13 presents a summary of the project, titled "Facilitating Sense Making for Situational Awareness." This research will focus on the development of algorithms and a software prototype for 1) the correlation of chat and structured data types and 2) the aggregation of data for higher levels of situational awareness. The technologies central to this research include data mining, text and information extraction, and data fusion.

Managing Information Goals

In the process of developing situational awareness (e.g., in accordance with either the JDL Data Fusion or Endsley models), opportunities to explore as-yet unexplored "regions" of a battle space may emerge. For example, the aggregation (or clustering) of data and the monitoring of these aggregations over time may suggest "hot spots" of activity, which, while not of immediate relevance, may be of future interest. In such cases, it may be worthwhile to allocate additional resources, either additional analysis or sensors (or a combination of the two), to one a hot spot. The issue of developing a suitable representation (i.e., a model) of a hot spot to support resource/sensor allocation then becomes an issue – that is, how does one develop a goal for information required in the future?

As an example of an opportunity that emerges from exploratory data analysis (which is, essentially, the activity described above), consider a MITRE direct-funded effort to develop data mining techniques to support U.S. Customs counter-drug intervention (Cabana, Babich, & Washburn, n.d.). In this research effort, the goal was to develop a set of "smart filters," which when applied to a large volume of air tracks, would allow an operator to focus on a particular subset of these tracks as "likely candidates" for an airborne drug-traffiker; that is, "targets-of-interest" (TOIs). Figure 14 illustrates the results of applying data mining techniques to a set of air tracks. Here, applying data mining reduces the number of tracks for further examination from the 200 produced by the track height-speed filter (blue font) down to 40 with a high signal-to-noise ratio (magenta font). While the nature of this particular problem allowed for the use of supervised data mining techniques (because historical data sets on airborne drug-traffikers were available), one could have worked this problem from an unsupervised viewpoint, "simply" looking for natural groupings in the volume of track data. In fact, one would not have begun the problem as a "problem," but rather as an exploratory data analysis task.

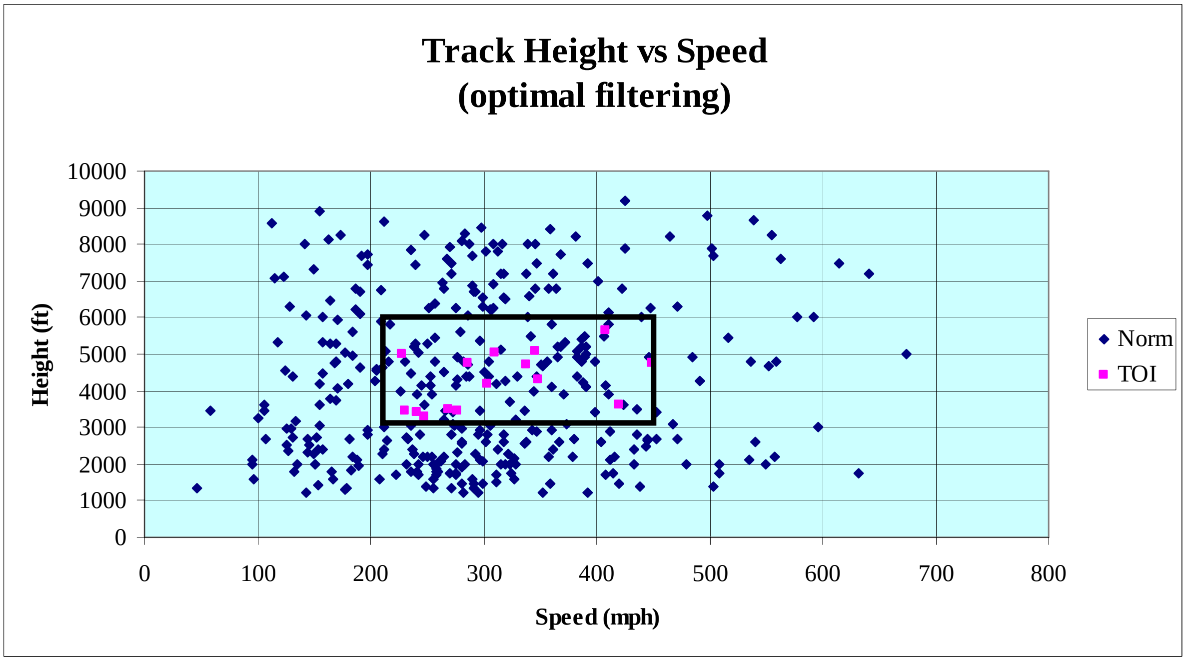

Figure 14: Using data mining to discriminate targets-of-interest in counter-drug intervention[7]

Exploiting (and Modeling) Complexity

While the recognition of complexity in certain aspects of military conflicts has been studied by a number of authors (e.g., Moffat, 2003), the recognition and exploitation of elements of complexity within an organization (i.e., an enterprise) appear to have received less attention, at least from a military point-of-view. Research conducted at the London School of Economics (LSE) in organizational complexity has concentrated on the study of an organization as a CAS. In particular, their research focuses on conducting "natural experiments" within organizations (e.g., BAE System, Citibank, the World Bank, and AstroZeneca). LSE has developed an integrated research methodology using both qualitative tools (e.g., interviews and narrative analysis) and quantitative techniques (e.g., agent-based models and simulation) to study organizations "open to change" (Mitleton-Kelly, 2003). Figure 15 presents the salient aspects of LSE's research program. Of particular note is the use of the visualization tool NetMap to establish patterns of connectivity using email exchange between elements of an organization.

An important problem in a netted sensors enterprise is the "optimal" allocation of sensor resources, in terms of their spatial and temporal distributions. Some recent research from the MITRE Technology Program (Mathieu, Hwang, & Dunyak, 2006) explores the application of biologically inspired distributed control algorithms to command and control problems. In

[7] From Cabana, Babich, & Washburn, n.d.

particular, this research has focused on the development of a "quorum sensing algorithm" to support target tracking based on the quorum sensing molecule (QSM), local interaction and nonlinear dynamics.

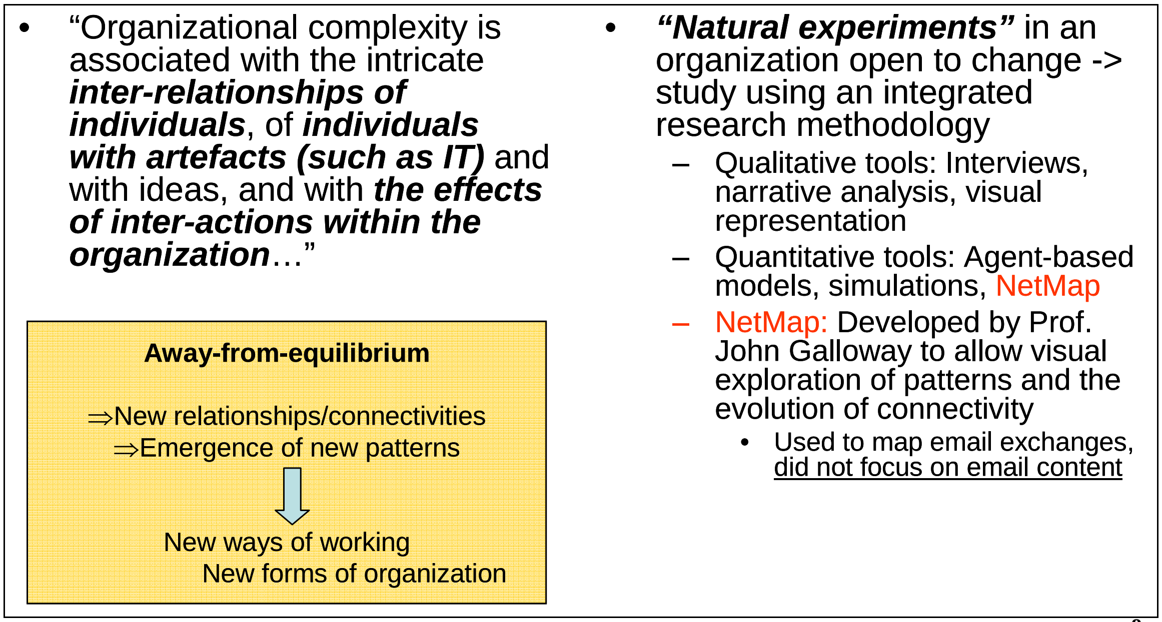

Figure 15: London School of Economics research in organizational complexity[8]

Figure 16 illustrates an example of the behavior of a QSM tracking algorithm in a netted sensors environment. The problem under study was one in which 600 sensors were randomly distributed within a spatial field, and whose job it was to detect a single target moving through this field to support a "down-stream" tracking function. Here, we see that the QSM tracking algorithm affects the activation of sensors (i.e., "Up-state Units") mostly within the "neighborhood" of the target of interest, where each sensor has a greater likelihood of target detection.

[8] From Mitleton-Kelly (2003).

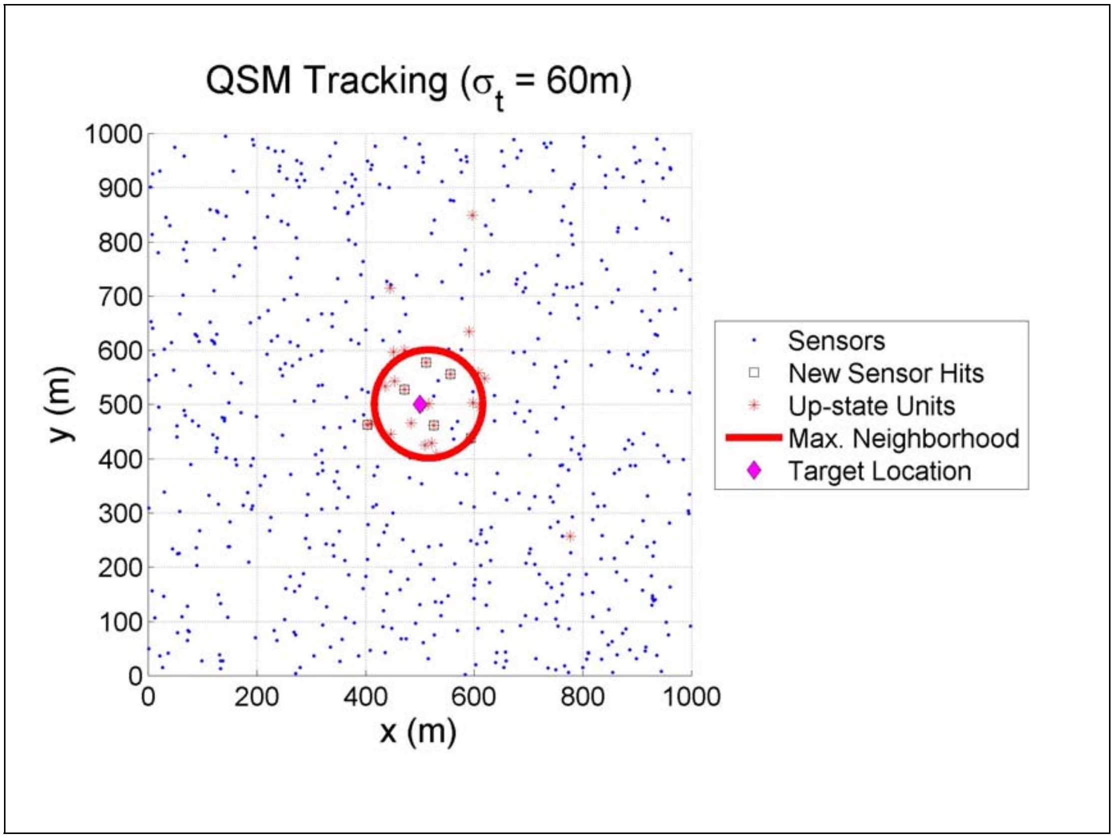

Figure 16: An example of quorum sensing molecule tracking of a target in a netted sensors environment[9]

[9] From Mathieu, Hwang, & Dunyak (2006).

3 Agile Information Management (The Right People and Time)

Introduction

Information Management comprises the designs, techniques and procedures that enable the "right people" at the "right time" to get the "right information"…based, of course, on the "right budget". Various processing, storage, sensor and especially network technology are employed to make information management more agile and better able to both handle stress and heavy load and adapt to potentially unanticipated new demands. This complex and dynamic environment requires rapid, on-demand information access where "right" is defined on the fly and may change unpredictably. Systems must interact in new and unforeseen ways at critical times of need with other information sources discovered on systems whose existence may only have been suspected.

The 'pull mode' concept of operations is no longer sufficient. Designers can no longer presume that operators will know a priori which source to utilize to get the necessary information. 'Push mode' support, where the sources generate information based on previous and current operator decisions, exploitation and usage patterns, must also be added to enterprise architectures and system designs.

Roles, group affiliation, availability and connectivity of network participants must also now be presumed even more dynamic than in the past. Flexible authorization and accounting mechanisms that can match dynamic organizations and their funding sources while maintaining attribution and audit trails will also be necessary.

With the increasing reach provided by networks, increasing awareness and analyzed options provided by processing and sensors and the sheer volume of information, now carefully stored, comes the threat of overloaded or misinformed decision makers and unreliable systems at a scale that challenges designers and operators alike. Complex Adaptive Systems can give warfighters and business managers alike an enduring and keen edge, but they must be handled with care and respect.

Information Management Tenets & Design Principles at the Enterprise Level

The tenets and design principles discussed below have been found useful in addressing the challenges listed above, but more importantly, they enable the enterprise engineer to leverage and exploit complex solutions to complex problems.

Composite Systems and Sources of Complexity

First and foremost, Complex Adaptive Systems result when systems are ***composed*** from distinct, relatively loosely coupled[10] components or modules. Component-based systems are significantly more robust and adaptable. The more loosely coupled the components, the easier they are to swap in or out on demand, as duly pointed out by enterprise system vendors such as IBM, who find it a compelling selling point, driving the shift from tightly-couple object-oriented components to more loosely-coupled web-service components (Bieberstein, Bose,Walker, & Lynch, 2005; Szyperski, 2003). However, the most prominent example of loose coupling in C4ISR systems is that between human operators and machines, as the old joke about the "loose nut behind the wheel" points out. Humans, in turn, are part of a larger Complex Adaptive System, geophysical space; the machines comprise cyber-space. A good part of information management design is dedicated to keeping the engineered systems and the living systems aligned with each other so as to apply resources in concert towards the intentions of the leaders.

Figure 17: Complex Adaptive Systems are Composite[11]

The simplest of the complex assemblages are more or less homogenous loosely coupled groups: grains of sand in a dune, a population of some species, and flights of micro-UAVs. Additional complexity occurs when diverse components are grouped: organisms composed of different kinds of cells, circuit boards, modularized operating systems and airplanes.

The first descriptive mathematical models of complex systems were stochastic. In particular, stochastic descriptions with heavy-tailed distributions (also called power-law distributions) are labeled complex. Stochastic methods are necessarily based on multiple samples. In the case of complex systems, the multiple components or participants that make up the

---

[10] Loose coupling occurs when two sub-systems only partially share their state spaces – a change in one doesn't *necessarily* result in a change in its neighbors. The result is a potentially non-linear system.
[11] Vitruvian Man: Leonardo DaVinci; NASA Flight Simulator: http://ails.arc.nasa.gov/Images/Simulators/AC97-0295-13.html ; Refinery: http://www.ca.sandia.gov/industry_partner/sensors1.html

composition are sampled during a finite interval whose length is defined by the lifetime of the target behavior(s) such that sufficient samples are collected to satisfy the modeling constraints. In this way systems can be captured even if they are short-lived ad hoc assemblages.

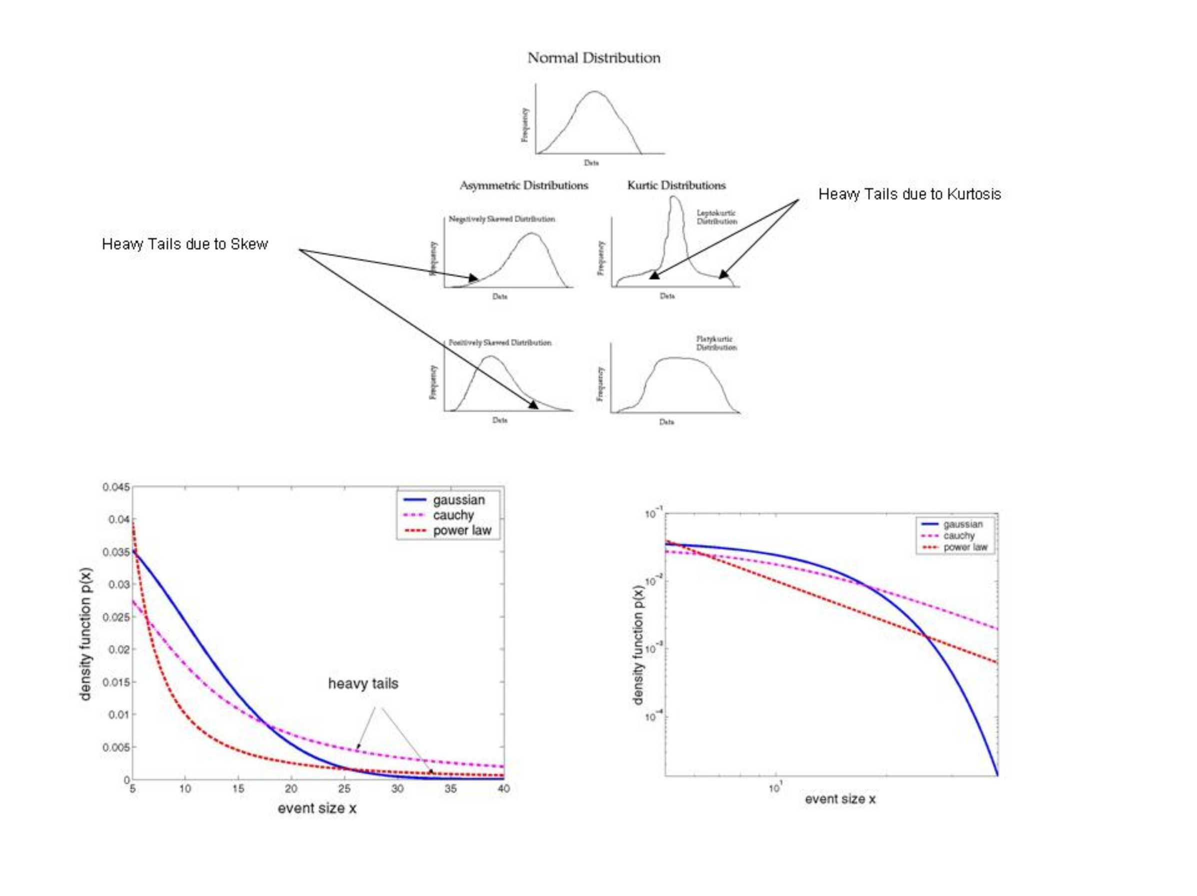

Figure 18: Heavy-tailed Distributions Indicate Complexity[12]

A number of causative mathematical models can result in heavy-tailed, descriptive distributions. Non-linear chaotic population models are the most famous, but there are also models in which the introduction of engineered linear components also cause the characteristic heavy-tailed distributions. Furthermore some otherwise rigidly specified and engineered systems can alternate between normal and heavy-tailed behavior. What, then, drives a system to be complex? In a phrase: *state space size.* What drives state space definition? The number of variables such as inputs and outputs, as well as their processing or

[12] **skew+kurtosis:** http://www.anselm.edu/homepage/jpitocch/biostats/normal.html [Prof. Francis J Pitocchelli] **linear & log:** http://www.physics.ucsb.edu/~mmanning/What_are_Power_Laws.html [Lisa (Mary Elizabeth) Manning]

relationships and the resulting shift to the next state. The most common way to formally describe a component is as a state machine that operates over a finite state space. The state machine of a component can either be discrete or continuous, depending on the coupling among the components, and the formal specification can range from probabilistic relations to differential equations.

Composite systems are systems that have distinct but interconnected components or systems of systems. They exist and operate at multiple scales, with one model for each component and another for the collection as a whole. Composite state space is an assemblage of all the potential states that are defined by the finite state machines of all the potential participants, whether human beings or engineered components. When the participants can exchange information, their behavior may coordinate. To the extent that their behavior is tightly or loosely coordinated, the components are referred to as *tightly-coupled* or *loosely-coupled.* In formal descriptions of these interactions, the participants are generally described in terms of their 'finite state machines', which detail what inputs result in what behavior and outputs. If several participants' state machines shift state in concert over a significant percentage of the combined state space – in one sense, their individual state spaces overlap significantly – they are clearly tightly-coupled. The less they act in concert, the smaller the 'overlap' and the looser the coupling.

State spaces can 'overlap' due to coupling in a number of ways, but the most common way to reduce the 'overlap' and de-couple is to grow the state space. State-space grows when there is an increase in:

1. the number of interactions due to increased number of simultaneous participants
2. the number of types of interactions due to increased diversity of participants
3. the length of the delay in inter-participant interactions beyond a certain threshold

Because composite state space is essentially combinatorial, an increase in any one of these factors can lead to at least exponential growth of the state space. As the state space grows exponentially, the ratio of the 'overlap' to the overall space drops drastically and the coupling shifts from tight to loose. In many systems, there is a threshold, one variant of which is described as 'period three' where this shift is extremely noticeable; to quote the famous article by Li & Yorke (1975):"it implies chaos."

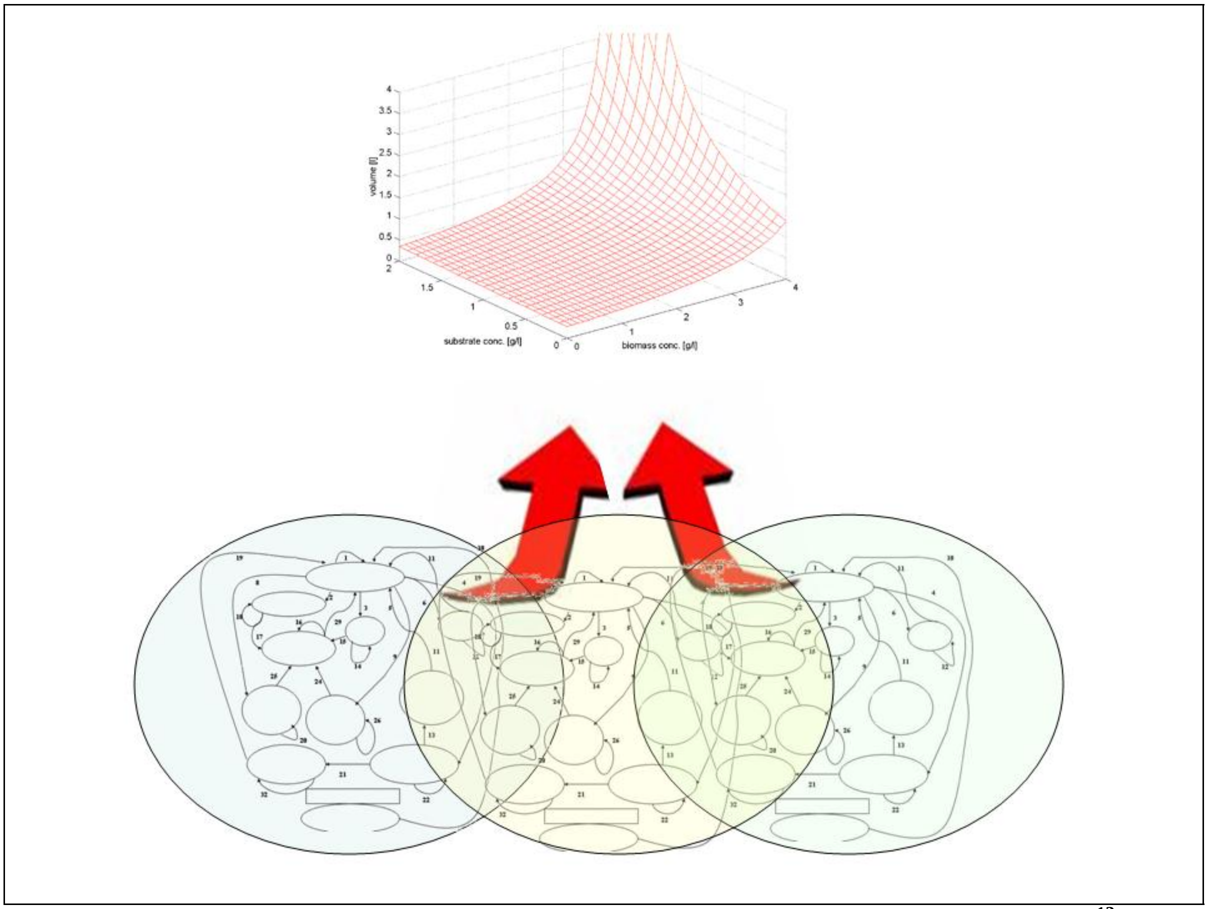

Figure 19: Complex System Composite State Spaces and Resulting Non-linearity[13]

Ironically, the result of such dramatic increases in state space can be an increase in the probability that the interacting participants will find their state machines dealing with second order, unanticipated synchronization – in other words, coupled through unexpected overlaps in a small subset of the state space, which means they are unexpectedly but loosely coupled. This is often a source of 'unintended side-effects' in human-designed systems.

Tight-coupling can also be unexpected in engineered systems; it is just much more likely to be detected, either on first inspection of a design or early-on in routine observation and thereafter it is an anticipated contingency. Furthermore, loose-coupling is not always bad; 'margin of error', 'over-engineered' and 'cutting some slack' are all well-known ways to effectively de-couple participants and increase the tolerance and reliability in anticipated environments. However, loose-coupling *does* introduce the potential for unexpected complex behavior, especially cascade failures, if the environment goes beyond the

[13] 3D Graph: http://www.ercim.org/publication/Ercim_News/enw56/hangos.html

anticipated and previously decoupled participants suddenly find themselves operating at the *bitter end*[14].

Managing Complexity in the Enterprise

There are numerous ways to manage complexity in any system, all of which involve reducing the number of states that need to be handled with the intent of *completely* decoupling all behavior except for a carefully-specified absolute minimum. In short, while attempting to manage complexity, enterprise systems engineers may introduce it unintentionally due to insufficient decoupling. While the average information systems engineer well understands minimizing unnecessary diversity and may even plan for large-scale numbers, very few understand the implications of introduced delay, especially variable delay. Almost none understand the cumulative effect of all these factors or how to assess and plan for crossing the complexity threshold in a normally well-behaved arrangement.

The upshot is a fair number of systems in which the people explicitly decouple themselves in self-defense from the engineered components, and when that is not possible, decouple the engineered components under their control from others and the engineered components are routinely labeled a colossal waste of time and money. This section describes various decoupling techniques when decoupling is appropriate, as well as how to specify and analyze coupling where it is appropriate. Appropriate coupling in enterprise information management enables effective performance by human participants and efficient performance by the rest.

There are a number of challenges introduced by even loosely coupling people and engineered systems into a large-scale enterprise. We call out four important ones:

1. Multiple orders of magnitude increase in potential information inputs – this results in the people in the system trying to "sip from a fire hose"
2. Orders of magnitude increase in the inputs to and speed of the decision-process, especially those that involve prioritizing and optimizing tradeoffs – e.g., where and when to bring resources to bear, what information is important, especially when the definition of 'important' is changed by a change in local or enterprise-wide goals
3. Orders of magnitude decrease in the control of technology due to looser coupling – the humans change from individual tool-user to a competitor or partner with others.
4. Different goals for the same human or system depending on what scope of the enterprise they are operating in. Within a scope they may be competitors, but when all the competitors are pushed into the next larger scope they must cooperate in order to survive in the competition against other coalitions.

[14] The very end of a line on a ship is tied to a *bitt* to keep it from losing it when all the slack is gone, but which when reached results in a great deal of sudden stress load on all concerned.

In order to minimize overload of the humans in the enterprise, there are a number of critical characteristics that must be present in the system engineering design. They enable the systems to track the humans as the humans adapt to changes. Normally these changes are caused by the humans (and their systems) shifting up and down the scope-scale, but changes can also be introduced by factors and forces that originate in systems and processes that may never be integrated into the larger enterprise, such as the natural environment.

The Five W Questions

In order to couple any two things, they must share *something* in common. Thus, ***orientation*** is the second most important tenet for operations involving complex systems. Its importance is emphasized in many analyses that characterize decision-making, such as the Observe-Orient-Decide-Act Loop. Much of the complexity in information exchanges about orientation can be summed up in four questions, implemented in the information management processes, procedures and other formal interfaces such as schemas. A fifth question conveys and adapts the leaders' policies via monetary and political capital control and feedback channels.

1. **What** – type, and instance
2. **Where –** location/access routing
3. **Who –** identity and role
4. **When –** time and coordination

and

5. **Why & Wherewithal –** intent & budget

By categorizing orientation information this way, humans can manage the complex information involved in orientation by organizing it into orientation schemas; the five W questions provide a generic template to be refined by a particular domain.

How to be Agile?

There is a sixth question that goes beyond the day to day operations the five "W" questions address. **How** to ensure that the designs, processes and procedures of information management enable a vigorous, long-lived enterprise? This requires agility, which we define as a combination of two strategic capabilities, redundancy and adaptability.

To align two systems at any one time, only a mutually agreed upon common framework is necessary; to align more than two systems or to align two systems across changing circumstances over time requires tenet #3a, ***standards*** for the orientation frameworks. Information management therefore requires a standard for each of the five questions. Five standards are needed for each type of space – living community or engineered. Standards enable *redundancy*: if a component or sub-system fails, then a replacement can be swapped in. Paradoxically, standards also can enable *adaptability* because they clearly delineate not only what is standard but which version of the standard it is and force discussion of migration approaches that allow the enterprise to dynamically evolve and not disintegrate.

This leads to tenet #3b, ***standard escape mechanisms***. Allowing for ongoing adaptation means covering even the outlier cases where the rest of the standard cannot cope and a replacement standard must be employed. Managing these unexpected cases happens more often in complex systems than random system models predict, and in life-or-death circumstances, having a built-in out can be vital. These escape clauses can be as simples as a free-text block or a placeholder URL that information providers can use to reference additional information. Whenever possible, these on the fly-extensions should be captured and analyzed so that the schema definitions can catch-up to these needs.

Information Management Tenets & Design Principles at the Large-Scale Enterprise Level

People familiar with engineered systems design undoubtedly recognize the above system engineering tenets – composition, orientation and alignment, and standards and standard escape mechanisms. There are other tenets that only come into play when dealing with extremely large scale enterprises. The complexity that entails from large scales is both a compensatory strategy and the target of constant information management concern.

Multi-Focal Organization: Coupling

The first enterprise tenet to keep in mind is ***multi-focal organization mechanisms***. Multiple organizational hubs facilitate three classic approaches to organizing large scale enterprises: sub-divisions, councils and hierarchy. Sub-divisions simply institute parallel local domains of control and coordination that enable expedited routine operations within each domain. Sub-divisions do not have to be imposed; they often arise from self-organization principles.

Coupling among sub-divisions can occur as interactions or communications between sovereign peers if the subdivision of resources is approximately equal, and coupling is relatively loose and coordinated effort only occurs if there is consensus. If the sub-division is not equal, communication occurs between levels of the resource division hierarchy, and coupling is relatively tight, with the superior delegating or loaning resources to and controlling the behavior of the subordinate(s).

However, whenever there is loose coupling, some information may be lost due to differences in resolution, delays in distribution, etc. Data Quality metrics are critical in dynamic environments where information producers and consumers may not have detailed foreknowledge of one another. These metrics allow information consumers to select information that best suits their needs and to make informed decisions. For example, information consumers may select information providers based on these metrics, and put-off decisions if information quality is low, or seek out additional information providers to verify or augment information.

Typical data quality metrics include accuracy, precision, completeness, and pedigree. Schemas used to describe data quality should be kept short and simple so as not to overburden information providers.

Multi-scale Organization: Encoding

Multi-focal organizations are complex only to the extent that the various centers are partially independent. It is that combination of independence and interdependence that makes them loosely coupled and the proportion of inde- to inter- dependence causes one of the most interesting complex characteristic of all: ***multi-scaled***. When a collection of sub-divisions is sufficiently coordinated in their behavior, they can be treated as a unit whose collective behavior is both more and less predictable.

To the extent that the coordinated behavior can be abstracted, hiding the gory internal details of the individual sub-divisions, that behavior is simpler to communicate across space and easier to remember across time because it is cheaper to encode. Encoding can be either in living members of the enterprise or the engineered systems that augment them. ***Multi-scaled encoding*** is the second large-scale enterprise tenet because it prevents complexity costs from overwhelming the resources available for coordinating effort.

Equilibrium and Organization: Modeling

Because we are dealing with composite, coupled systems, their components can be perturbed by external forces. Such perturbations can disrupt coordination and force different adaptations within different sub-divisions, redistributing the balance of resources and capabilities. Managing a complex enterprise not only requires information management for diverse and dynamic resource and information flows, but also ***large scale equilibrium modeling*** such that the humans do not feel overwhelmed and the engineering is computationally tractable. This last tenet is one of the hardest to implement because the mathematics is non-linear, probabilistic and heavy-tailed. Such mathematical territory is typically avoided by traditional engineering disciplines.

Below, we propose a strategy to address this by looking at how the classic four questions of systems information management, augmented by the why, wherewithal and how of classic operations information management, are transformed by multi-focal organization, multi-scale encoding and equilibrium models to create agile enterprises, suitable for the growing range and scope of situations we are facing.

What and Where is the Right Information?

To provide information management that supports the needs of a complex, adaptive enterprise, several key information technology enablers must be in place. In dependency-order they are:

- *Standardized Loosely-coupled Domain Definition* – the first enterprise pre-requisites are the will, authority and budget necessary to determine a common *why* and *wherewithal*; these in turn define a community or domain both in geophysical space and cyber space. At extremely large scales, these often will be self-organizing; under certain circumstances the structure will be self-similar (fractal) as well.

- *Standardized Loose Coupling Meta-data for What, Where, When, Who* – at very large scales due to multi-focal sub-divisions there will be both hierarchical and federated standards processes. Local communities should ensure that they have properly credentialed delegates for all hierarchical standards authority and properly selected representatives to all relevant federations. Procedures whereby the standards can be ignored so that variants can be tested, competed, and evolved are critical.

When developing semantic formal community models, operators and systems should expect to share information with parties that are unknown to them during design and development. This has several important implications for developing and documenting formal semantics models:

- Semantic models must be made accessible. This means they must be captured and published using standard forms that are machine-readable

- Semantic models must be as free as possible from implicit definitions and assumptions; source context information can be used to flag any potential conflicts in definitions and assumptions. A “tank” from an Armor unit’s Lieutenant on the ground might be flagged by software and double-checked by a coalition Airman coordinating fuel deliveries, even though fuel capacity is common to both armored tracked vehicles and storage facilities. Of course, a General’s armored tracked vehicle might indeed be getting an airlift special delivery.

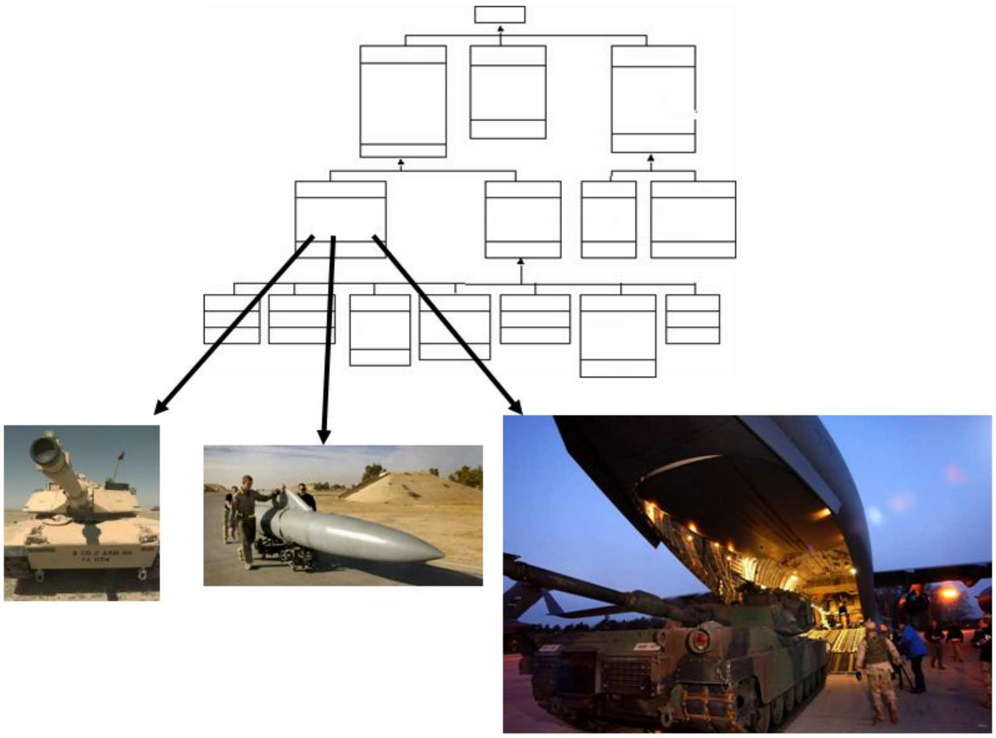

Figure 20: Deconflicting Diverse Enterprise Semantic Modeling[15]

Semantic models should focus on the meaning of the data and allow for diversity in format. Alternate representations tied to underlying semantic models allow for information to be tailored to the needs of specific operator and communities while maintaining data interoperability.

When developing semantic models, flexible processes should be used to find good-enough solutions. Given the requirements of a complex, adaptive enterprise, it is no longer feasible or advisable to put extensive processes in place that are laden with committees and checks and balances. Searches for optimal solutions should only be undertaken when there is ample time and the environment is stable.

Many schema management standards delegate responsibility for low-level context services to other standard enterprise-wide services. Name/Authorization mapping is generally handed

[15] **army tank:** http://www.fas.org/man/dod-101/sys/land/m1.htm
F-16 fuel tank: U.S. Army photo by Staff Sgt. Timothy Lawn [http://www.af.mil/photos/]
C-17 loading Army tank: U. S. Air Force photo by Master Sgt. Dave Ahlschwede [http://www.af.mil/photos/]

off to the Lightweight Directory Access Protocol (LDAP) identity service and the Name/Address mapping to the Domain Name Service (DNS).

Simply understanding information exchanges can be useful, but real situational awareness only comes with coordinating information generation or discovery across multiple team members. Likewise, real capability only comes with coordinating information exploitation. Coordination requires coordinated real world context information – clocks must be synchronized, a common translation between geo-spatial datum agreed upon, and an organizational identity and authorization (clearance and classification) model agreed upon.

Likewise, in the supporting information management universe, agreements must be negotiated for virtual clock/counter synchronization, address assignment management and routing convergence, network identity management and crypto key exchange methods.

Finally, both the real organizational world coordinated mechanisms and the network virtual world coordinated mechanisms must be aligned through the use of:

- *Adaptable & Redundant Information Distribution* that ensures the distribution of information in a highly dynamic, time sensitive environment where network connectivity is at risk or network infrastructure is heavily loaded. Build-out and configuration of distribution networks in very large scale environments is already primarily machine-to-machine, but only in response to acquisition and capital budget life-cycles, not decision loops or changing operational situations.[16] In addition to distribution of operational information, there are a number of shared information infrastructure capabilities that themselves need adaptable information distribution. At very large scales, this means the efficient machine-to-machine access to and distribution of advertisements of publication and search engine functions. At large scales, machine-to-machine access to and distribution of meta-data directories and registries, and data catalogs are also needed.

- *Dynamic Information Discovery* that ensures user and systems can find the right information not only at design-time, but at run-time as well. This means that at very large scales machine-to-machine discovery mechanisms are required in order for the right information be accessible at the right time.

- *Adaptable & Redundant Data Mediation* that ensures information can be understood and interpreted across the enterprise, even when there are different standards due to different domain focal points. Since the second major source of delay is information access authorization and redaction, this means that at very large scales machine-to-

[16] Consider containerized shipping and telecommunications service; both tend to build out large transport infrastructure networks based on aggregated capital cycles, then retail standard capacity at the edges according to retail capital cycles. Acquisition of on-demand capacity requires first setting up either a retail pre-paid or billing account which is periodically rendered according to retail capital cycle standards.

machine mechanisms that are well integrated with distribution mechanisms are needed for information assurance. Unfortunately, due to certain complex system self-organizing principles, these integrated facilities often create more complexity in the process of fulfilling other needs. This makes it a fertile area for research, and there are a numerous ongoing efforts, primarily in the areas of dynamic mapping among structured data schemas and adaptive redaction and intrusion detection (Lin, Risch, & Katchanounov, 2002; Sampada et al., 2004; Tzitzikas & Meghini, 2003, August).

Focus on Information Exchanges and Communities

There were several attempts to create a single common vocabulary across the Department of Defense, the DoD Data Administration Program being just one example. The promise of these efforts was that if everyone used the same data model for representing and storing their information, then data interoperability would be assured. These efforts failed to fulfill this promise for many reasons, including the difficulty in reaching and maintaining agreement of such a large-scale vocabulary involving a multitude of organizations. Two important lessons learned from these efforts are:

- The complexity of reaching and maintaining semantic agreement is a function of the amount of information that must be agreed upon and the number of organizations that must reach agreement.
- How organizations and systems represent data internally is of little consequence. What is of importance is the meaning and structure of their information exchanges.

The current DoD strategy states that semantics are to be managed within sub-divisions known as Communities of Interest (COI). A COI is defined as a group of users and stakeholders "who must exchange information in pursuit of their shared goals, interest, missions, or business processes and who therefore must have a common vocabulary for the information they exchange." COIs are simply a formalization of a sub-enterprise scope.

Adaptive Information Access & Distribution Services

The concept of Network-Centric Operations and Warfare (NCOW) envisions an environment where information is posted before it is processed, information is available across the net, and information consumers can discover and access the information in a timely and reliable fashion. The effective machine-to-machine (M2M) sharing of information across a network is essential to the realization of this vision and the ultimate success of our military operations. Without it, decision loops lengthen, situational awareness suffers, and the quality of available information is lower.

Network-centric drivers and enablers are those network-based architectures and network technologies that improve adaptability to these conditions and enable continuity of operations where previously there would have been a brittle failure. High bandwidth, low delay communications are technically harder and more expensive, *but* by shifting from point-to-point communications to networked communications the enterprise can take advantage of the *network effect* driver: costs go up only linearly while intelligence sources and assets available for coordinated information exploitation go up exponentially.

The resulting shared higher bandwidth and lower delay communications enable richer potential information exchanges that cover a wider range of contingencies. Planning and configuration values may become minimally compressed information copies, not highly-compressed pre-planned *references* to information; this enables a wider range of coordination using un- planned information. Remote planning and coordination can also draw on a larger pool of assets now accessible through the net, and there is exponentially wider situational awareness and intelligence.

However, the network-centric M2M sharing of information is made much more difficult by the very dynamic environments in which the Air Force, as well as its Joint and Coalition partners, operate in. Thus, we cannot predict in advance who will need to interact with whom, communications paths may be unreliable, systems and operators may be unavailable for periods of time during operations, and needs for and uses of information will change.

Several capabilities are critical in enabling adaptable and reliable network-centric M2M distribution of information in the AF range of environments:

- Information providers and consumers must have a range of methods for describing their information capabilities and needs in an environment where a range of network capacities and information assurance capabilities are encountered during information distribution.

- There must be decentralized methods for consumers to identify information providers that best suit their needs, since information selection and prioritization become critical when there is a wealth of potential information providers.

- There must be a reliable information exchange capability that can adapt to changes in network connectivity and availability of participants. In support of this, there must be capabilities to find alternate routes across a network when portions of it have become inaccessible. Further, information must ultimately reach network participants even if those participants were unavailable when the information was originally sent. And information must be scaled to a variety of resolutions to support the needs of participants at the edge of the enterprise distribution network, including mobile participants operating in limited-bandwidth environments.

Some of the technologies and techniques particularly useful for distribution across loosely – coupled components and through domain boundaries are:

- Peer-to-Peer Protocols

- Broadcast & Multicast Distribution Protocols
- Intelligent Agents
- Intelligent Distribution e.g., content-based, location-based
- Transport-aware and Storage-aware Data Protection services

Adaptive Information Discovery through Search Services

Traditionally, information providers and their content are discovered and integrated at design time. A developer identifies the content and information services that their application requires and then constructs the necessary interfaces to access that information. As a result, changes to a consumer's information requirements require that changes be made to the application, the information provider, or both.

To provide true adaptability in the face of changing information requirements, information discovery must shift from being a design-time activity to a system-mediated run-time activity. Systems must be able to search for and access information providers that meet their changing information needs. Before the tighter coupling that defines a particular COI develops, or for discovery outside of and between COIs, the following technologies and techniques are useful:

- Broadcast/Multicast/Advertise protocols
- Intelligent Agents
- Ad hoc and Natural Language Search Queries and Filters
- Protection-aware Search Access

Adaptive Information Discovery through Catalog Services

Once a COI reaches a certain level of maturity, intra-COI discovery can be standardized. This requires that information providers publish rich, machine-readable descriptions of their information and services, and that information consumers have efficient and reliable access to the underlying registries and catalogs. The following technologies and techniques are applicable:

- Service Oriented Architectures
- Subscription Protocols
- Semantics and Ontologies
- Orchestration and Workflow Management
- Protection-aware Lookup & Browse Access

Adaptive Information Mediation Services

Mediation services bridge semantic gaps in the enterprise through space, across eras and between political sub-divisions. At very large scales these need to shift from design-time data mediation to true M2M run-time mediation. Like Information Discovery, these fall into two categories, depending on how mature the community's standards are.

First, in order to communicate with mature communities, the data must be encoded in a common format. Humans must use the same alphabet or characters to represent the concepts; machines likewise must also negotiate to the same representation encoding.

In order to communicate meaningfully, the data must be distilled into a common, mutually negotiated vocabulary. Mature COI vocabularies and representation encodings include well-known standards such as defined by the Simple Mail Transfer Protocol (SMTP), those found in unified ontologies such as OWL and MIME, and those referenced in federated (context-sensitive) ontologies such as RDF. Run-time mediation can also support model & schema extensions as long as the *process* of assigning a data type to its referent can be standardized within the community.

Useful technologies and techniques in use among mature COIs include:

- Ontologies
- Semantic Web
- Distributed Metadata Negotiation & Management
- Conceptual Modeling techniques
- Language Translation services

If there is a mismatch between the structural richness in data encoding or vocabularies due to maturity, legitimate differences in operational resolution, summarization, compression or redaction in response to austere communications resources or protection policies, additional technologies and techniques come into play.

- Emergent Pattern Analysis based on inferences about What, Where, When, Who obtained from raw sensor-generated information context.
- Distributed Data Quality and Stewardship based on export & import policies for process-generated information.
- Transport-aware Data Encoding services
- Protection-aware Redaction services

When is the Right Time?

There are two aspects of time that are important to C2ISR operations. The first is in establishing one of the foundations of *rate*, especially rate of resource consumption, rate of approach/retreat and frequency of event occurrence. Monitoring or controlling any process over time requires two types of time specifications or time meta-data: the measure or clock and the reference timeframe. The first determines the baseline method of sequential changes that establish the units and continuity of all other rates in the system. The second determines the scope and scale to which that baseline applies.

In a large enterprise, especially one that is based on a coalition of peers, there may be multiple time sources or clocks and associated timeframes. ‘Synchronizing watches’ and the world time zone standards are two classic examples of methods of aligning timeframes.

Clocks & Time Sources

There are three main types of clocks: the original diurnal sun-clock, the current atomic-decay clock and the network-centric virtual clock. The first two are used in geophysical timeframes and drive coordination of resource usage and physical interactions based on a locally monotonic sequence of physical events. The third is a logical construct used to drive coordination of discrete event systems based on locally monotonic sequences of virtual event dependencies (Lamport, 1978). In all cases, dynamic systems are by definition rooted in the timeframes defined by their clocks.

Geophysical Timeframes

Geophysical timeframes are important in an enterprise because not only do they have an inescapable direct impact on mass and energy resources, but also because they are generally politically defined with the associated direct legal impact. They also have an indirect or second order impact because they define movement, and movement defines locality in a dynamic system and locality defines the probability of interactions. Assets, entities and resources that are nearby are more easily closely coupled since there are more potential communication channels and more potential opportunities for both competition for local resources and collaboration in the face of local problems.

A third order impact can be created by modulation of a rate of change, which can be used as a means of signaling or communications. An entity that shares resources that increase its consumption may become a potential competitor. One that decreases its consumption decreases the potential for competition. If such increases or decreases mirror neighbors’ consumption patterns and follow them closely in time, it may be possible to infer their intentions (Malle & Knobe, 2001).

Network-centric Timeframes

Network-centric timeframes are defined by virtual clocks. Although there are also geophysical clocks used in network-centric operations, they are exclusively used to coordinate geo-physical entities and processes through the network. Timing sources are used to synchronize physical layer signaling, generally in the service of human sensory requirements such as the transmission of voice, video and remote control. Administrative timestamps are used for legal and political coordination in network-centric operations and management. All else may use geophysical clocks but only as a convenient source of ordinal numbers for labeling sequences.

Time Scales and Complexity in Decision Making

Every time-based interaction has its scale defined by its native or natural ‘clock’. Many of those clocks are second- or third-tier, subsidiary chemical or engineered measures based on either solar or atomic processes. Therefore there will be multiple time scales simply because there are multiple, coupled oscillators.[17]

Delivering information ‘at the right time’ usually means ensuring that it arrives within an interval which enables decision makers to exploit it effectively and efficiently. Such intervals are defined by combining the availability of resources used in the decision process, any delays in transport and storage, the attention span allocated for processing the information, the availability of resources used in the exploitation, and finally the availability of exploitation opportunities. Machine multi-variable calculations of ‘the right time’ therefore require meta-data that is both timely and time-aligned. Because such contributing factors are often cyclic, there are often multiple ‘right time’ solutions of varying efficacy and efficiency, so computational effort becomes another factor in ‘the right time’.

Who are the Right People?

Sharing information requires that both the provider and the consumer be the right people. *Rightness* has several information management reference frameworks: political, geophysical, and network-centric. In most cases the geophysical location of the people and equipment defines the political and network-centric reference boundaries and membership identity.

Ex Officio: Roles, Identity & Clearance

The concept of a *role* evolved because individual entities cannot always be on active duty and because humans have capabilities beyond those that they use for a particular job. Roles enable agility in the form of robustness from load-sharing and failover and adaptability from escalation procedures and differential training. The system shifts from individual to individual among a group while fulfilling a single role; the individuals shift from role to role as they pursue their goals within systems. To the extent that the role can be formally defined, it may benefit from machine-to-machine support or even automation. Identity, therefore, exists on three planes: the individual identity on the geophysical plane, the individual identity on the information space or network-centric plane, and role identities that formally define information management capabilities. Clearance is a declaration of fitness of an individual to comply with information assurance requirements while operating in a role; it must map the individual identity to the role identity. Consequently, all identity sub-systems in an enterprise information management system must deal with all four kinds of identity data, including:

[17] Note that loosely coupled oscillators exhibit one of the first analyzed forms of complex behavior.

- **Geophysical Identity –** This material identity reference framework is the essence of most traditional political and legal systems. Sovereign nations are based on interactions within a geographical scope; human organizations such as corporations are based on interactions among the people that compose it.

- **Network-centric Identity –** This information identity reference framework is based on the geophysical framework because the expenditure of energy to encode, process, transport and store information is directed by a geophysical entity. Mapping between first order information space virtual entities to the corresponding geophysical entities constitute a large part of identity management systems because it enables one first-order entity to locate another.

- **Role Identity –** Roles are a way to create an adaptive, robust information space identity. They map a second-level or abstract virtual entity to multiple equivalent first-order virtual entities. Shifts can change and people and material assets can be replaced, but the role's operational capabilities have continuity.

- **Authority to Clear, Authority to Classify –** Authority is the last of the 'Who' collection of meta-data because it binds the control of resources to identities. At its most simple level, geophysical identity represents a single entity's authority and command of material and energy assets – the warm body, in personnel terms. Network-centric identity at its most simple level represents a single entity's authority and command of information and intelligence resources. The authority to control usage of the material and energy assets or control access to the information assets is a foundational interaction with other entities. That *classification* control information is often implicitly captured in 'Who' identity information – shared assets are often represented by shared identifiers. The authority to declare that another entity is trusted or *cleared* for otherwise restricted access is encoded as identity information, either implicitly as shared identifiers or explicitly in an access control binding like a PKI certificate.

Identity Information Management Services

How far to extend trust is simple at a single scale: trust all members of your local scope, don't trust non-members. However, due to the principle of sub-division, at enterprise scales both material and information resources must be imported and exported to both peer scopes at the same scale and to superior or subordinate scopes at different scales. Representing how far the trust extends is a key aspect of information management's identity management sub-systems. It must be able to represent *delegation* for the export of authority, and it must be able to represent *pedigree* for the importance of authority.

Standard interaction information types or *meta-data,* such as identity, delegation and pedigree meta-data, are necessary for two identity management sub-systems to support export/import interactions necessary for mission command or coordinated effort. When two identity sub-systems interact they also need to align their authorities by exchanging authority delegation and pedigree meta-data about their identity information. This process, known as *authentication*, is fundamental. To the extent that information is duly bound to delegation and pedigree meta-data there is *transparency,* as each participant knows exactly who has done what to whom within each scope at each scale.

Multi-scale authority information represents a chain of trust that crosses scopes and scales. The Public Key Infrastructure (PKI) is an open information management standard for trust chains. It defines a trust scope as the realm of a server that stores identity/authority information, enables machine to machine cryptographic authentication methods, and provides a management capability that allows authority information to be created, updated, retired, and distributed. It supports multi-scale trust chains by encoding authority as a hierarchy of PKI scopes, where each scale derives its identity (and implicitly authority) from its parent scope.

Information Assurance

However, in going up or down scale, authority information is often deliberately lost. Superiors take credit (and responsibility) for their subordinates' efforts. New information is often generated by aggregating information from other sources, but the organization and exploitation of that source information is not performed under the authority or responsibility of the source entities. Privacy and redaction requirements also require either loss or masking of identity information. Finally, in very large enterprises, the identity, delegation, and pedigree information soon grows to the point that it may completely outweigh the content it describes, and in austere environments this burden may not be justified. All scope boundary information management systems (e.g., next generation firewalls and automated guard cells) must be able to review and prune multi-scale identity, delegation and pedigree meta-data, as well as the mission content data, in support of these information import/export capabilities.

Which is the Right Budget?

Technology solutions are necessary, but not sufficient, for information sharing. To fully realize the benefits of robust information sharing, the socio-economic barriers to information sharing must also be addressed. Many of those socio-economic forces are managed through budgets, so information flows in an enterprise are those enabled by corresponding financial investments and those whose credibility and reliability are backed by solid funding. We offer the following tenets for building incentives for information enterprise information sharing:

- Acquisition processes must address information sharing by identifying the overarching principles and concepts of operation that rely on sharing and call out to what extent sharing will be implemented through shared infrastructure constructs, including networks, shared processing, storage, and servers. A more detailed review of which information management components constitute infrastructure is in the sub-section on Information Infrastructures below.

- Program managers must be given incentives to build information sharing capabilities into systems that enable information flows both internally and for sanctioned export and import.

- Information providers must be given incentives to share information. Providers often fail to share information out of fear (of providing the wrong information or making some other mistake) or greed (holding onto information and requiring others to come to them increases their perceived power).

Information Management Risk/Cost/Benefit Analysis

Information Management should mirror the human organizational structure, which in turn mirrors information generation and exploitation decisions. Information Management often uses system architectural constructs to implement policy boundaries and cost/benefit tradeoffs. Some of the principles and forces that drive the analysis and the resulting structure are:

- In a network-centric information sharing, the benefits go up as the square of the number of [*constructive*] participants – Metcalfe's Law, [O'Brien's extension]
- Costs go down inversely to economies of scale and number of competitor providers – Adam Smith
- Risks go up as the square of the number of *destructive* and *obstructive* participants – O'Brien's Law

The initial investment to share information via a network has several parts:

- Initial Threshold or Barrier to Join:
    - Capital equipment acquisition costs
    - Space & Environmental acquisition costs
    - Integration costs
    - Training costs
    - Increased Risk of Discovery through the network by opponents

- Ongoing Costs of Operations must also be considered; many sales emphasize low acquisition costs and hide subsequent operational costs
    - Space & Environmental Leases
    - Power & Communications Service Costs
    - Increased Risk of Exploitation or attack through the network by opponents

However, in a network-centric environment, the benefits can increase exponentially while the financial costs only increase linearly. Common network effect benefits available immediately include:

- Increased access to larger resource pool
- Improved diversity of resources that can be used to adapt to unexpected situations
- Improved situational awareness due to discovery of others, both friend and foe.

Ongoing network sharing benefits include:

- Shared infrastructure costs

- Continued adaptation capabilities due to diverse resources that enable ongoing continuity of operations
    - Improved on-the-job training due to additional opportunities to observe models and mentors
    - Network-centric automated resource exchanges:
        - Resource Market-making
        - Reciprocal Service Agreements

The Impact of Increased Information Sharing

The social dimensions of enterprise information management are not confined to sharing issues. Integrating machine-to-machine sharing into an enterprise enables such major improvements in the availability, freshness, and cost of information that it can change concepts of operation and decision-making procedures. Such changes in operation change the acquisition requirements for the system components, with the overall result being enterprise transformation. The areas of social impact -- areas that commonly undergo transformation -- are those that improve the ability to

- export appropriate information quickly and cheaply
- coordinate operations across previously un-bridged operational boundaries quickly and cheaply

By improving the speed of interactions and associated information exchanges, and making it easy to reduce the information exposure, trust can be built incrementally and easily between partners

Robust Information Management

Earlier sections discussed various adaptive approaches. They included a range of information packages based on varying distribution capabilities, decentralized information sources, use of search capabilities to find previously unrecognized information sources, and mediation capabilities to enable their usage.   This section covers making information management robust, that is, able to react constructively to change and challenge.

Redundancy Mechanisms & Issues

The classic response to a robustness requirement is to add capacity – make it stronger, make it more powerful, make it larger. Also known as 'over-engineering', 'redundancy', and 'margin of error', the immediate issue is to balance the tradeoffs between the costs of producing "more" and the expectation that the "more" will be needed. In the network-centric information space, adding more translates to *redundant material* components and *replicated information* components.

Whenever there is redundancy or replication, the immediate issue is selection – when and how do the replicated resources come into play? The answer depends on the scope of resource management, which is determined by the coupling between the generic resource and what determines its usage. When a superior sub-system draws on a tightly-coupled set of subordinate replica resources, for the resource selection process is not visible externally. The only external impact will be that the superior sub-system can cope with a wider range of operating environments or offer a firmer guarantee of service. However, in a network-centric enterprise this is not the only kind of coupling, and looser coupling means the selection mechanism is externally visible. One of the most common network-centric information management capabilities is to provide local replicas of distantly produced information. By decoupling the query process from the distribution process, local consumers receive more reliable access to fresher information with lower delay. This is not only useful for mission information services, it is critical to robustness and performance of enterprise information infrastructure services such as catalogs, directories and search engines. In short, information management system robustness depends on robust distribution combined with robust storage mechanisms.

Robust distribution primarily depends on redundant network channels – a set of chains of transport resources that can convey information   Selection of a particular channel may be internal if the distribution is within a local scope, but anytime information management must traverse a boundary, the distribution channel needs an individual usage interface that actually conveys the information and an overall management interface used in the selection process. If more than one information flow shares the channels managed by the selection process, the selection process must also manage capacity and arbitrate usage.

Likewise, robust storage depends on redundant information copies. . Selection of a copy may be internal or external, and administration of shared storage must manage and arbitrate usage.

Robust information management also requires multi-scale information assurance aspects. If replica selection is externally visible, then an attack on one replica may cause a failover to another in a clearly visible way. However, if the replication is hidden at a lower scale level, attacks of an underlying replica can trigger a 'silent' failover. If the replicas are so similar as to have the same vulnerability, then the next replica also will fail. Eventually the failover mechanism will come to the end of the chain of dominos, and the fault will propagate up to the next scale. If the next scale up is likewise replicated, attacks on all of the underlying scale components will cause a massive surge of failures to hit the upper scale failover mechanisms almost concurrently, resulting in an unexpected surge that often brings down the whole enterprise in a cascade failure and gives rise to the idea that such engineered systems are brittle.

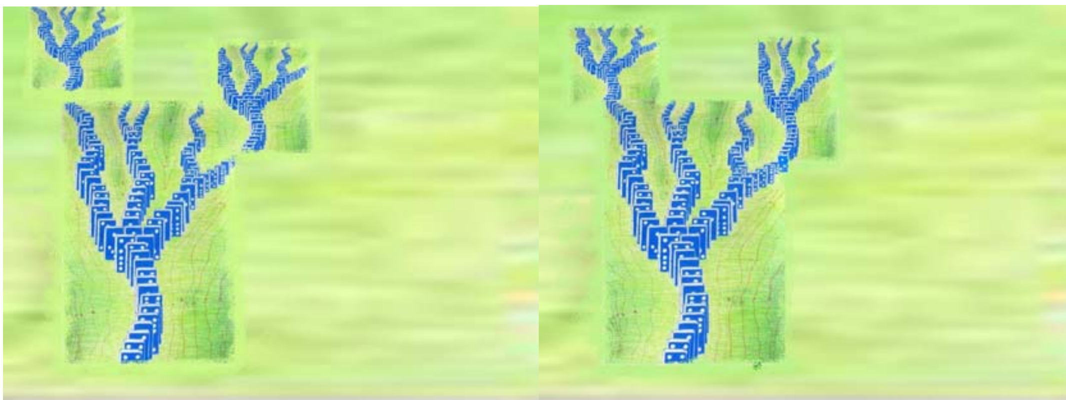

Figure 21: Multi-scale Systems are Vulnerable to Cascade Failures[18]

Such multi-level surges are not planned for primarily because of the way technology investment decisions are made in large scale enterprises. Accounting domains are replicated to match the sub-division of labor, and the aggregate accounting may or may not exist, depending on the legal organization and accepted rules of accounting. The larger the scale of the enterprise, the less likely there is to be an overall accounting and the more likely that the risk/cost/benefit calculation will only take into account local risk levels. The risk of cascade failure typically falls below the threshold that affects decision-making (otherwise, better replica management would be at least considered). The other factor is that until recently most investment decisions did not take into account either the *Law of Large Numbers*, or the fact that the kind of underlying but hidden interdependencies cause failure-risk likelihood distributions to be heavy-tailed. The combination means that such failures will occur much more frequently than traditional analyses would predict.

Adaptability Mechanisms & Issues

True agility requires not just robustness, which can result in brittleness as we've demonstrated above, but also *adaptability*, which is the ability to change strategies by changing the *type* of resources, not just change out the particular instance currently deployed. When applied to information management, this principle results in three main families of tactics:

[18] Based on "The Domino Effect", Nicholas Grivas, Decatur, GA, [(c) River of Words; http://www.riverofwords.org/gallery/2004/22.html]

- **Adaptable Information Distribution –** Ensure the distribution of information in a highly dynamic, time sensitive environment.
- **Dynamic Information Discovery –** Ensure that information about information sources is visible to the right people well before they need it.
- **Adaptable Data Mediation –** Ensure that visible information is also provided using encodings, structures, and terminology that the local infrastructure can handle, and ensure that local consumers understand how to make sense of the differing semantics.

It also requires corresponding adaptable collateral services:

- **Adaptable and Scalable Information Assurance –** When new information sources are used, command authority and protection mechanisms must automatically adjust accordingly.
- **Adaptable and Scalable Funding –** When new information sources are used, financial authority and budget transfer mechanisms must automatically adjust accordingly.

Information Infrastructures

Sharing Resources: the case for infrastructure

The most important factor in determining an information infrastructure implementation construct is that no single entity can afford the {time/money/skills/people} to provide that utility alone. Consequently, solving the common problem requires coordinated action and creates stakeholders.

If the service can be broken into component parts and each stakeholder can take responsibility for a part, then they collectively benefit from each other's contribution. This model would not impact the current standalone system acquisition model so long as each standalone program of record adopts the standards that ensure their part will interoperate with the others. This is the approach advocated by NESI (Net-centric Enterprise Solutions for Interoperability, see http://nesipublic.spawar.navy.mil/).

However, this “lots of little parallel efforts” approach requires that competition among the stakeholders be managed to minimize the tendency to create parallel standards. More importantly, there are whole areas of infrastructure that cannot be done in parallel but are best done as standalone “utility company” programs. In such cases the worries come not from standards (the utility company enforces de facto if not de jure standards), but from ensuring that the utility services truly meet the needs of a sufficient number of stakeholders.

Evolution of Infrastructure

Implementation constructs often evolve from co-ops to corporations quite naturally -- that's how the Internet has evolved -- so any acquisition process should focus on "future--proofing" the service standards so that they can be governed both ways. As Internet operations evolved, the micro-services were developed and deployed in parallel under a co-op governance process known as the Internet Engineering Task Force and InterOp. Macro-service bundles later evolved based on bundling micro-services into corporate business packages and products. Unfortunately for acquisition organizations, the commercial private sector has developed past the micro-service level, and they are now primarily concerned with selling macro packages that enable them to at least attempt to monopolize the market. Sometimes there are 'natural monopolies' -- distribution networks offering transport services are the most famous example, and DISA is the DoD "utility company" organization.

Enterprise Infrastructure: End-to-End Key Interfaces Profiles (KIPS)

There is a need to identify key micro-service interface profiles that will enable macro-bundles that have taken up residence in operational nodes to interoperate. The following list identifies the ones found to be critical in getting value from a working and workable commercial Internet composed of a combination of organic NESI-node-like and utility-company stakeholders.

- Distribution Services
- Distributed Time Service
- Distributed Network Identity/Location Mapping & Location Discovery
- Distributed Organizational Identity/Network Identity Mapping, Authorization Mapping & Discovery
- Distributed Basic & Extended Web Services
- Distributed Business Services

Allowing global end-to-end KIPs also turns out to be critical to future-proofing because it allows new services to evolve naturally as a collection of micro-services within an early adopter co-op community and then shift gears into corporate mode and macro-service packaging.

Enterprise Service Development & Governance

GIG-E micro-services will always need parallel co-op development and acquisition because they have to be "installed" in many nodes that are often termed Service Access Points, mechanisms, clients or agents. The crypto-based authentication and authorization handshaking mechanisms are a classic example. Network stacks, management agents and discovery clients are three more (think Winsock, SNMP agents, LDAP clients, browsers).

GIG-E micro-services that are AC/DC are power, the original bi-modal infrastructure (DC stores and does long-range transport best, AC does retail operations best), information transport (LAN vs. WAN) and identity (Local vs. Global addresses/labels). Note, truly mission-critical utilities are almost forced to be switch-hitters because you can't always depend on the utility company to deliver.

GIG-E micro-services whose macro-bundles can be highly optimized (more on this definition another time) are natural utility company services. In this space are long-haul distribution networks (material, power, and information), storage farms (storage area networks, and some server farms) and enterprise distributed processing (other server farms and grid computing).

Enterprises need both an inclusive infrastructure strategy and a spectrum of governance procedures for all service packaging approaches. At one end are the processes, KIPs and guidance needed for network-centric node development and at the other the processes, KIPs that focus on *inter-node* information distribution. The latter highlights the micro-service boundaries between macro-bundle implemented nodes. However, defining that interaction only as a single macro-bundle like the Enterprise Service Bus (ESB) is insufficient and worse, prone to failure because of too many parts, too many of which are 'moving' (active). Even relying on ESB within your node may cause critical information exchanges to fail because of intra-node service dependencies & failures, such as occur during distributed attacks from bots & worm. Multi-level defense means each individual system needs to have backup service providers, if only a cache of the remote server’s state; worst case a service consumer needs to be able to make progress based at least on local information.

In addition to checking macro-bundle interoperability (ESB to ESB) interoperability testing processes need to check that systems gracefully handle failure of each and every underlying micro-service (duly identified in the KIPs), plus KIP combinations as identified in standard macro-service implementation constructs.

Information Management Use Cases

The use cases selected for this section focus on the two critical elements of an agile information management function: a sufficient architecture for this capability (and its leveraging of web services), and the types of patterns needed (ontological; other) to ensure the legitimacy of information moving broadly across the enterprise.

Dynamic Information Management in Complex Enterprises

Adaptable and reliable information distribution is essential to effective decision making. Effective information distribution is complicated by the complex, dynamic environment that the Air Force and its partners operate e.g., network participants may be unavailable at times, communities of Interest and their memberships will be fluid, and communications may be lost. The goal of this research area is to investigate an enterprise information distribution capability that combines the strengths of peer-to-peer and publish and subscribe technologies to share information in near-real time while being adaptable to changes in its environment. The prototype resulting from our research will be applicable to a wide variety of areas to improve information sharing including battle management, collateral damage assessment, and blue force tracking.

Semantically Enabled Web Services for Effective Decision Making in Network-Centric Environments

Given the momentum of Web services and services-oriented architecture and the early state of semantic web technologies and ontology modeling, it is important to evaluate the value of adding semantics to Web services. This research area applies the semantic web concepts of the WSDL-S approach to a selection web services and will evaluate this approach and its effectiveness for enabling and improving the automation of web services discovery, composition and mediation, reuse of web services and the flexibility and re-configurability challenges of using web services.

Managing Infostructure Complexity in Agile Decision Support

This research area expects to refine a mathematical model based on characteristic parameters of both decision-making information flows and information technology systems. Using the model as a base we intend to produce an initial prototype decision aid that takes these classes of parameters as input, generates contours representative of the interface between decision information flows and technologies, and matches requirement contour to capability contour. The model concepts (and the tool that enables rapid 'what-if' scenarios) can be used by infostructure designers and managers to rapidly model and evaluate potential infostructure re-configurations. Such evaluations will not only establish overall acquisition requirements and but also to adapt the systems in the field. Use of the model concepts and of the tool enables standardized (and ultimately automated) policy-based re-configuration specifications whose contents can be coordinated across multiple platforms.

4 Agile Information Exploitation (The Right Decisions)

Introduction

The previous two sections discussed the role of agile information generation and management in the C2 Enterprise. In this section, we address another critical link in the chain: exploiting that information to support enterprise capabilities such as decision making, situation assessment, course-of-action selection, and resource allocation. We define information exploitation as ***"the interaction of technologies and human cognitive and collaborative processes enabling sufficient sense-making and situational awareness for agile, effective decision making."*** Information exploitation refers to the direct use (explicit or transparent) by people of these functions and underlying technologies as well as the appropriate collaborative processes to make decisions. The Exploitation function is based in Cognitive Science and Collaborative Information technologies, and pays strict attention to how people best function under complex decision making situations, and how technology and processes can best be integrated to support them.

Effective decisions are the end products of successful information exploitation. And since humans are ultimately responsible for making decisions by exploiting and adapting the capabilities of systems in the C2 Enterprise, we advocate that systems must be designed with adequate consideration of the role of human operators, teams, and their mission objectives. Moreover, we advocate that systems engineers should construct systems that amplify and augment human cognitive strengths and help overcome human limitations. Technology should support the needs of the warfighter, not vice versa: in effect, people and mission objectives become the "forcing function" for technology. We need to move beyond the design philosophy of "Science Finds, Industry Applies, Man Conforms" to the philosophy of "People Propose, Science Studies, Technology Conforms" (Norman, Things that Make us Smart).

Thus, the central information exploitation challenge is to confront the issue of **Human-System Integration (HSI)**. HSI is a comprehensive strategy to optimize total system performance (e.g., humans working with machines), minimize total ownership costs, and ensure that the system is built to accommodate the characteristics of the operators (e.g., their strengths, limitations, and biases) who will ultimately operate, maintain, and support it (311 Human Systems Wing, Brooks-City Base, TX). Some of the central issues of HSI include how to determine the information to display to operators, how to format the information display so it is congruent with operator goals and decision-making objectives, how to effectively distribute tasks across team members and technology, and how to determine when a system is usable, effective and leads to greater performance than either people or technology could achieve working in isolation.

Some would argue that the basic problem in C2 of complex systems is that error-prone humans are simply inadequate to handle the rigors of decision-making along with the vast amounts of available information, and "with just a little more automation we can eliminate the 'human error problem' entirely" (Christoffersen & Woods, in press). But the fact is that an enterprise is a complex interaction of people (e.g. soldiers, commanders, etc.) and processes, as well hardware and software systems, and people will always be central players in enterprises because of their sense-making skills, creativity, expertise, and adaptability. This is particularly so as the line between systems acquisition and systems operation is blurred by human beings who are constantly adapting themselves and their systems to meet emergent and unexpected challenges of dynamic battlespaces.

In the remainder of this section, we outline a strategy and associated research needs for moving in a direction that will allow us to make the best use of information, people, and technology in large-scale, distributed cognitive systems (enterprise systems).

The Information Exploitation Environment

The increased complexities of future C2 environments pose ever greater demands on the need to quickly and accurately exploit information. There are a variety of characteristics of the information exploitation environment that complicate effective operation. Below, we relate how these complications affect information exploitation in particular.

A Dynamic and Complex Battlefield

The battlefield environment is one where new information is constantly coming in, old information is invalidated, goals are changing as situations evolve, and decisions are made in real-time in response to such evolving conditions. Moreover, decisions are never one shot events. Rather, a series of non-independent decisions are made that change the state of the battlefield, and it is only possible to judge the quality of a series of decisions in retrospect (Thunholm, 2005). The complexity of the battlefield environment means that the critical function areas of information generation, management, and exploitation must be tightly coupled and integrated. That is, decision makers must have access to the current state of the battlefield to determine the impact of their decisions, a capability provided by information generation. They must also know where to find such information and be able to access it rapidly, which are capabilities provided by information management.

Increased Volume and Rate of Information

In the C2 Enterprise, vast amounts of data and information are available from a multitude of diverse and distributed sources. This increased volume and rate of information available to decision-makers has the potential to lead to more-informed and therefore better decisions, but it can also lead to information overload. Decision-makers may spend an inordinate amount of time determining which information is relevant to their goals, attempting to make sense of that information, searching for additional information, and making a decision based on the totality of that information. Moreover, decision-makers must also deal with the trade-off between waiting for near-perfect information before acting, or acting more quickly with "good enough" information. However, the rapid pace of future battles and the need to stay within adversarial decision loops will punish those who procrastinate (Alberts, 1996). Thus, information systems must support decision-makers in developing rapid plans by conveying when the amount of information backing a particular decision or course-of-action is "good enough." Information fusion techniques discussed in Section 2, including Bayesian updating, can go a long way in extracting the maximum amount of utility from available information. And techniques discussed in Section 5 that aid operators in developing flexible and robust plans, rather than potentially brittle optimal plans, can also be of use.

In addition to getting the *right information* to the *right people*, information must also be in the ***right format*** so people can make the ***right decisions***. Determining the proper format and display of information must be based on both decision making goals and human cognitive and perceptual strengths. People excel at recognizing patterns, matching patterns to past experiences, and selecting courses of action that were successful in the past (Klein, 1999). We shed light on ways to effectively present information to operators in sections on *Cognitive Engineering* and *Decision Support Systems and Automation* below.

Reduced Manpower and Cost Goals

Across the Services there is a push to do more with fewer personnel and less cost. Secretary of Defense Donald Rumsfeld has advocated making changes to transform the military into a "leaner and meaner" force capable of winning "every single battle that this military is faced with." The Office of Naval Research's Science and Technology Manning and Initiative has set as its goal a "fifty-percent personnel reduction while demonstrating operational utility for all functions. Thus, there is a need to design systems that maintain acceptable levels of performance with fewer people.

In order to meet these reduced manpower and cost goals, the role of the human has largely shifted from more narrowly specified missions to multi-mission tasking, and from manual control of a single system to supervisory control of multiple and possibly automated systems. For example, rather than five operators controlling a single Unmanned Aerial Vehicle (UAV), it is likely that in a future scenario a single operator will supervise a fleet of five or more semi- or fully-autonomous UAVs. However, careful consideration must be made of the roles and interactions of the human and machine elements, and automation should only be introduced when there is a specific need to do so (Mitchell, Cummings, & Sheridan, 2004). The subsection titled *Changing Human Roles* below highlights the concerns that must be addressed to ensure effective human-automation collaboration and coordination.

Changing Human Roles

Due to the increased volume and rate of information, as well as the increased operational tempo brought about by Network-Centric Operations and Warfare (NCOW), operators will be increasingly called upon to supervise and utilize automated support systems to assist them in decision making tasks. They are also confronted with different types of missions and concepts of operations, such as multi-mission tasking, the trend towards decision making at lower echelons, and Distributed Operations in which small, highly skilled and independently-operating units must aggregate quickly to provide sufficient capability wherever it is required against a complex and adaptive threat. Given the importance of human insight and adaptability for these new roles, the goal should not be to replace human expertise with automation, but rather to amplify and augment it.

Many current automated systems simply provide "optimal" decisions without providing insight into the reasoning behind the decisions or leveraging operator expertise. However, several unintended human factors and system performance problems arise from such an approach. For one, it is impossible for designers to predict and model every situation in dynamic and complex battlefields, so the "optimal" decision may not always be optimal or even correct. This lack of robustness, or brittleness, is a key reason for keeping flexible and creative human operators in the decision making loop. For another, systems that do not allow operators to rapidly understand how a system came to its advice may cause automation bias, where operators either place too much trust in the system solution when they shouldn't, or place too little trust when they should. And when operators have little insight into the operation of an automated system, their situational awareness is degraded.

To counter these problems, we believe that automation should allow operators to rapidly understand the reasons and results of automated solutions, adjust system parameters and assumptions as conditions change, and visualize and explore problem spaces so that they can leverage their sense-making skills, creativity, adaptability, and expertise to overcome the problems of automation brittleness and bias.

High Stakes, Time Pressure, and Uncertainty

The battlefield is a high-stakes environment where errors may have serious consequences. Moreover, operators are often under extreme pressure to make decisions as quickly as possible where there is much uncertainty and ambiguity. Such high stakes, time-pressured, and uncertain environments may lead operators to adopt decision making short-cuts (heuristics) and biases that information system designers must be aware of. While such strategies are generally effective, they can also hinder decision-making in situations where they lead to systematic biases (Mitchell, Cummings, & Sheridan, 2004). Relevant heuristics and biases include:

- Anchoring and Adjustment Heuristic: People make an initial guess about the likelihood of a particular event or battlefield state (e.g., I am 80 percent certain that track is an enemy tank), and they adjust their assessment based on new information (e.g., the track is traveling over rough terrain, so now I'm 85% certain that it's an enemy tank). People run into problems because they generally don't make sufficient adjustments to their initial assessment. Systems that employ Bayesian techniques can help people make more optimal adjustments (Burns, in press).

- Availability Heuristic: People judge the likelihood of a particular event based on what has happened in the recent past or what is most readily “available” in their memory. This can be problematic when the current event differs from any recently available event. Systems that maintain a history of past events and assess their similarity to the current event can help overcome fallible human memory.
- Representative Heuristic: People often evaluate probabilities based on the degree to which A resembles B. One side-effect of this heuristic is the “conjunction fallacy,” where specific scenarios appear more likely since they’re representative of how we imagine events. However, specific scenarios are mathematically less likely than more general scenarios.
- Confirmation Bias: People tend to seek information that confirms their initial assessment and discount or explain away disconfirming information. Thus, there is a need for information systems to support people in considering multiple possible assessments and selecting the most probable assessment.
- Automation Bias: People may place too much or too little trust in solutions provided by automated systems. This is particularly true of automated decision support systems whose reasoning is not well understood by operators.

There is a need for information systems designers to be aware of these heuristics and biases and develop systems that exploit their benefits without performance degradation. For example, systems must display uncertainty so operators can calibrate an appropriate level of trust as contexts change. There is a need for further research in ways to effectively communicate and represent uncertainty in a manner that is coherent to operators and enhances decision making. Bayesian techniques may help people reason under uncertainty and extract the maximum utility from available information (Burns, in press).

Information Exploitation Challenges

To develop a strategy for effectively leveraging information, people, and technology, we must first identify the major challenges for information exploitation within enterprise systems. An understanding of the underlying challenges will allow us to develop a set of corresponding information exploitation tenets to guide systems engineering efforts.

People Steer, Guide, and Supervise the “Engine” of Technology

In relatively stable decision making environments, technology has been a powerful driver of human decision processes and functions. For instance, automation of a task that had been time-consuming, tedious, or error-prone, can enable people to adjust their roles and associated allocation of time and effort accordingly for better performance.

But in complex enterprise environments where threats and associated priorities change unexpectedly, this technology-driven approach fails. Information exploitation becomes a highly dynamic activity, requiring continual sense-making and adaptability. The human decision makers become the forcing function, since it is people who can apply their expertise, perspective, and contextual knowledge for higher-level sense-making and detection of unanticipated cues in the environment. Just as we would temporarily suspend our car's automated cruise control when we notice highway congestion ahead or the start of inclement weather, dynamic and complex environments require a different type of interaction and feedback between people and technology for high performance.

People provide the experience and perspective to detect cues that a course correction may be needed, e.g., instances when seemingly valid and reliable system information no longer makes sense within the current context and thus violates an existing information pattern. They can initiate activities to determine whether the disconnect stems from the system information itself (such as an input error, faulty algorithm, or information *from* the wrong source or sent *to* the wrong recipient), or is due to a perception of the environment that is no longer accurate (e.g., the type of threat, desired effects, or resource constraints have changed). To support this "helmsman" role, systems must provide feedback on the external environment, in addition to feedback on progress towards specific ongoing tasks. Technologies such as data mining may greatly assist in this role by identifying *potentially* important patterns within vast amounts of data, after which human insight and sense-making are essential for determining those changes in pattern most likely to be truly significant within the operational environment.

> **Tenet 1**: Provide feedback on surrounding context to facilitate detection of changes in underlying patterns.

> **Tenet 2**: Design for "re-directability" of technological resources.

As discussed in Section 1, an important feature of an enterprise is its dynamism. That is, an enterprise is in a constant state of evolution, reinventing parts of itself through a process of continual innovation and integration. Successful navigation through such an environment requires near continual monitoring and characterization of that environment with an eye towards detecting any significant shift in patterns. (See also Section 2, "Monitor for Change.")

> **Tenet 3**: Enable more *continuous* monitoring/characterization of the decision making environment.

Moreover, effective human system integration must enable people to readily communicate any significant shifts in environmental patterns via changes in parameters of the supporting systems. Based on a detected change in the environment, systems may need to immediately begin monitoring different information sources or scanning for new patterns. Technology can greatly speed information sharing, task completion, and overall performance once the appropriate tasks and direction are identified, but there is a greater need than ever for the "human in the loop" to perceive when the course of action must be altered: "We're making great progress, but in the wrong direction!" People perform these essential roles of sense-making and adaptability, and apply their insights to complement and steer the supporting technologies. Although we continually strive to reduce manpower requirements and the forward footprint, our efforts to automate must focus on tasks that are more stable, rote, time-consuming, and/or error and bias prone – but not those calling out for human sense-making, insight, and innovation.

> **Tenet 4**: Leverage and amplify (versus replace) human experience, insight, and adaptability.

In these complex environments, people are also taking on more Human Supervisory Control (HSC) roles over increasingly autonomous systems and vehicles. This involves explicitly supervising and guiding technologies (such as UAVs), intervening when performance is unsatisfactory and then relinquishing control back to the system when its performance is again stable. Systems must be designed with this human-machine interplay and dual feedback in mind; they must provide operators both the system performance information and sufficient contextual information for the necessary sense-making we described. This becomes particularly important as we ask people to maintain supervisory control over *multiple* systems and vehicles.

Dynamic information acquisition, filtering, and tailoring

R4 is the goal of getting the Right Information to the Right People at the Right Time to make the Right Decisions. But a critical challenge for information exploitation within enterprise systems is that the "right" information cannot be fully specified in advance; it is situational and dynamically determined. Addressing this challenge requires synergistic efforts between information generation, information management, and information exploitation, as depicted in Figure 22.

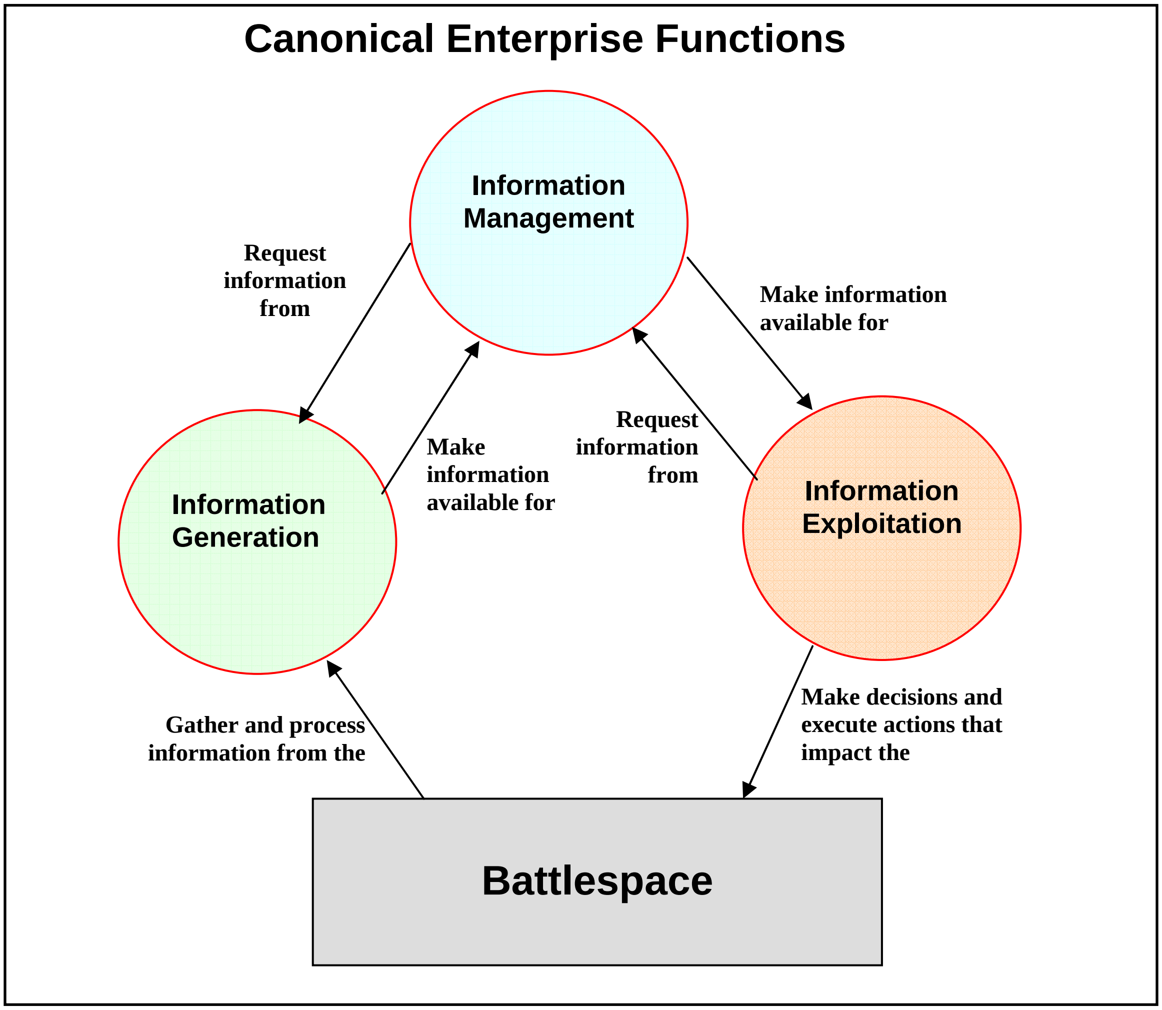

Figure 22: The canonical enterprise functions

For example, in confronting asymmetric threats and more agile adversaries, the kind of information that can be exploited to our advantage may be of a new type, in a previously unseen format, or from a new source. This means decision makers must have an infrastructure for information *acquisition* that allows them to modify their information needs in real time (see Section 2 on Agile Information Generation). The information *management* function must similarly allow them to combine information, filter information, and enable desired push or pull mechanisms as a need is identified; operators will be unable to fully describe all information needs in advance (see Section 3 on Agile Information Management).

> **Tenet 5:** Link information generation, management and exploitation efforts to enable dynamic extraction of the "right" information.

Decision makers also contribute to the assessment of the information's source, pedigree, trustworthiness and reliability before they act on it; systems should provide contextual meta-data to facilitate this process. Since ambiguity is the rule rather than the exception in complex enterprises, determining information provenance is particularly important and challenging (see also Section 2, "Make Explicit the "Quality" of Data or Generated Information at All Levels").

> **Tenet 6:** Facilitate *human understanding of* and *inputs into* determination of information pedigree, provenance, and trustworthiness.

Moreover, users must be able to locate the required information within their decision cycle or it loses its value. To quote Cdr John "Nano" Nankervis, USNR, OIF Chief of ATO Production, "Unknown capabilities are the same as not having any." Since operators are typically bombarded with vast quantities of data, they currently bring informal social networks, as well as information technologies to bear in order to locate the necessary information or expertise. Unfortunately, while experienced teams often develop highly effective social networks and information management processes to assist their exploitation, newer teams without those established relationships, processes, and skill sets may have great difficulty locating and exploiting the relevant information in time. They require both technologies and processes to facilitate this agile composition of needed resources and expertise, as well as mechanisms that permit them to dynamically and adaptively filter, set alerts, and tailor displays without undue effort or delay.

> **Tenet 7:** Value and facilitate information *accessibility*, beyond its existence.

Operators Use of a Multitude of Disjointed Systems and Communications Modalities

Operators must often make use of a variety of systems and communication mechanisms to accomplish their decision making tasks. As Enterprise Systems Engineers, we must not only consider the impact of a specific system on operator performance in decision making tasks, but also how that system will interact with other systems the operator may be using. The introduction of a new system may overload operators and hinder their ability to work effectively with existing systems to accomplish tasks.

For instance, Internet chat has become a pervasive communication modality in military settings, and operators often monitor half a dozen or more chat windows while simultaneously communicating with collocated team members. Operators monitoring a number of communication threads often become cognitively overloaded ; people have a limited attention bandwidth and simply cannot attend to each system with the same level of concentration. Thus, careful consideration must be made of how the introduction of a new system will impact operator cognitive load and attention management. A deep understanding of operator tasks is necessary to ensure adequate integration of a new system within an operator's suite of systems. Automated attention cueing strategies, filtering techniques, and the integration of disparate systems or displays into a cohesive system more suited to an operator's overall set of tasks are potential solutions,

> **Tenet 8**: Design and introduce technologies with awareness of the actual work context, including interactions with other systems being used simultaneously.

Not only do operators rely on a multitude of systems, they often also rely on multiple *modalities* (such as phones, radios, headsets, public address systems, email, instant messaging, or face to face discussion). Multiple modalities may be needed to communicate with distributed team members and enable the necessary feedback and coordination for real-time team-level exploitation and response. Observation of operators within an AOC (Boiney, 2005) revealed that operators not only have to determine *what* information to focus their attention on and *with whom* to share it, but also must make countless secondary judgments about *how* to do so: what means of communicating will provide the desired response most effectively?

For example, an operator could post information to a designated database or shared application, in which case it's likely other team members will know where to "pull" the information from if it's needed. Alternatively, the operator might "push" the information via face to face discussion or by phone, which guarantees that the intended audience receives the information but provides no persistent record of the communication and does not scale to more than a few people. Instant messaging is another possible means of information sharing, in which case there are decisions to be made about the appropriate chat room(s) to address, or whether a *chat in private* directed at a particular individual would be more appropriate. Yet another option is to use *audio* chat over operator headsets, in which case the operator's comments will be immediately heard by the selected individuals, *if* they are present. Teams employ these various modalities differently, depending on the importance and time-sensitivity of their communication and the intended audience.

> **Tenet 9**: Design and introduce technologies to support information exploitation within the multi-modal communication environment.

Before any new communication modality is introduced, its utility in meeting operator goals and decision making tasks should be clearly understood. The efficiency and effectiveness of a particular communication mechanism should be evaluated against other potentially better communication mechanisms, and in terms of the overall impact on performance when used in conjunction with other modes of communication.

> **Tenet 10**: Automation should decrease, not increase, cognitive load in complex enterprises.

Moreover, training should guide operators in how different communication mechanisms should be employed, individually and in combination, to meet different decision making goals and objectives.

> **Tenet 11**: Train as you Fight; Fight as you Train.

Distributed Collaboration and Operations in Complex Environments

Operators in the C2 Enterprise do not perform their tasks in isolation. Rather, they work in teams that may be collocated or distributed across geographical boundaries. Thus, teamwork and collaborative decision making are critical components of the military's vision of network centric warfare, which is becoming an integral part of current and future military operations. A basic tenet of networked forces is allowing individuals and/or groups the ability to leverage information both locally and globally to reach effective decisions quickly. Collaboration is both a critical element of networked operations and of military operations in general, and with the increasing trend of automated sensor and weaponry technology being introduced in these environments, successful battlefield operations will involve effective collaboration between not only humans, but also humans and automated systems (Scott & Cummings, 2005).

Information exploitation is a collaborative activity, requiring teams of typically dispersed individuals to share information and perspectives, coordinate activities, and reach shared understanding in order to make decisions. Increasingly, collaboration crosses boundaries of service, agency, and country to form highly heterogeneous teams with Joint, Coalition, Cross-Agency, or even Military-Civilian membership. As a result, teams must achieve shared understanding and shared situational awareness in the face of different incentives, cultures, perspectives, and constraints. While a cross-agency team may share unity of *effort*, they may not have unity of *command*. This often means that consensus building, resource allocation, and other decision making must rely on the ability to *influence*, rather than to control. Moreover, in highly complex environments characterized by emergent threats (such as Homeland Defense and Security scenarios), the composition and formation of the team itself becomes dynamic: the "right" people and corresponding resources are not fully known in advance, but rather must be assembled in real time. This poses additional challenges for information exploitation, since the set of decision makers who must share information, coordinate activities, develop trust, and reach shared awareness may never have worked together before. Complicating matters still further, the team's membership may continue to evolve as new areas of expertise are required.

> **Tenet 12**: The "right" people in R4 is also dynamic; enable information exploitation across heterogeneous teams with changing membership.

Another challenge of collaborative information exploitation relates to the sheer quantity of connections between people and systems. As we move towards network-centric warfare, we are gaining the ability for anyone, anywhere to communicate with anyone else. Yet effective information sharing necessitates *selective* information sharing to avoid overload. Because there is so much information coming from so many sources in so many forms, and because it is being processed, interpreted, and updated by many systems and people, operators currently report that it takes experience and informal social networks to know where to look and what you're looking for (Boiney, 2005). One of the key findings from observations at JEFX 04 was that more links do not equal more or better coordination. There are costs associated with additional links and interconnections that translate into system latency, information overload, and an inability for people to manage their attention effectively across the plethora of systems, communication modalities, and individuals transmitting information.

> **Tenet 13**: Enable *selective* information sharing to balance the need for good judgments with the risk of cognitive overload.

> **Tenet 14**: Value more understanding over more information.

In addition to garnering sufficient situational awareness, teams must develop sufficient awareness of the team itself – including others' identities, roles, activities, and status on tasks. For effective coordination and collaborative information exploitation, they must know something about what others on the team know – and do *not* know – at a given time, whether they are present at their stations at the time of critical communications, and how busy others are. Without these types of Team Awareness, people may share information inadequately or excessively, misinterpret a response or a delay in receiving one, and lose trust and/or shared situational awareness. Maintaining team awareness is challenging in distributed environments since people can not readily see or hear one another. It can exacerbate information overload as operators strive to understand *who* they're dealing with and who's doing what, in addition to *what* is going on around them. In such environments, teams currently rely on a mix of technologies, such as tailored coordination displays, phone calls, and instant messages in order to stay abreast of others' activities; no single technology currently addresses this need.

> **Tenet 15**: Provide mechanisms to maintain awareness of others' activities, knowledge, and load ("team awareness) to enable effective coordination.

Trust Formation

Establishing appropriate trust among decision making entities is crucial to ensure agile and effective information exploitation. Issues of trust pervade all elements of the information exploitation environment: trust must be established not only between humans and technology, such as decision support systems and information sources, but also between human team members. Interpersonal trust plays a vital role in people's willingness to share information, as well as their ability to collectively validate incoming information and resolve differences of interpretation when the information is contradictory or unclear. For example, people are continually vetting information as it arrives, judging its relevance, provenance, pedigree, and trustworthiness. Some of these attributes are inferred based on the *human* *sources* of information, and their perceived credibility, competence, commitment, and motivation. In time-pressured scenarios, the absence or presence of interpersonal trust and credibility can be the determining factor in which opinions and inputs get full consideration. In short, lack of trust is a potential socio-cultural “show stopper” for effective exploitation and decision making.

To enable appropriate levels of interpersonal trust, team members share much more than directly task-related information. Collaborative information exploitation requires rich interpersonal communication for some issues, and technologies to enable these less obvious but equally important drivers of communication. Different forms and modalities of communication – such as email, chat, VTCs, and machine to machine posting within systems of record – will be appropriate for certain types and purposes of communication, and potentially detrimental for others. For example, a team may be able to communicate most of the technical information via an online briefing with accompanying audio. But periodic face to face or VTC-enhanced discussion may be imperative at key intervals to ensure there is an opportunity to detect social cues, develop relationships, and establish buy-in. This is particularly important if the team is distributed and heterogeneous; it takes significantly more time and effort to establish trust and cohesiveness across organizational boundaries, since corresponding team members will typically not be co-located, not know each other well, and not share all of the same goals, values, priorities, procedures, and social or cultural conventions (Boiney, 2005).

Both the development and the *implementation* of these modalities (e.g., training, tactics, techniques, and procedures) must be designed with an awareness of when and how they can aid information exploitation.

> **Tenet 16**: Provide both *systems* to enable social, trust-enhancing interpersonal communication, and *processes* to guide their appropriate use.

Co-Evolution of People and Technology: Performance of the Joint Human-Technological System

Both human cognition and information technology are necessary for effective information exploitation; the goal must be complementarity, combining and augmenting the strengths of each, rather than substitution. Operators *adapt* both their processes and their use of technology to meet emergent, unexpected needs. Many researchers have noted that although systems are typically designed with specific uses and purposes in mind, people will appropriate those tools in whatever way best suits their goals and needs.

> *People are “purposive, knowledgeable, adaptive, and inventive agents who engage with technology in a multiplicity of ways to accomplish various and dynamic ends. When the technology does not help them achieve those ends, they abandon it, or work around it, or change it, or think about changing their ends”* (Orlikowski 2000, p.423).

Secondly, the introduction of technology *necessarily* changes human cognition, behaviors, and interactions. This is evident even with relatively simple technological interventions, such as the shift from face to face communication to the use of email or chat, in which the sender's attitude and intent must be – sometimes erroneously – inferred. The introduction of technology can result in unintended emergence in which the interdependencies between multiple systems and human processes create undesirable consequences. For example, we discussed earlier how enabling widespread connectivity between individuals and teams who were previously disconnected (or limited to communication up a restricted chain of command) unintentionally lead to information overload. New technologies should be developed, trained for, and assessed with an awareness of these inevitable impacts on human cognition and behaviors, and with the goal of developing appropriate guidance and processes to maximize intended emergence and minimize unintended emergence.

> **Tenet 17**: Emphasize and assess the performance of the joint human-technological "cognitive functional system."

In dynamic and complex environments, technologies often force workarounds (or get abandoned) because they were designed for a relatively stable and predictable information exploitation environment. They expertly and optimally implement a specific series of tasks, in a particular order, yet are too brittle to withstand the adaptations that will be needed for fluid information exploitation. One of the reasons that the use of chat has exploded in operational settings is because it is easy to use and designed for general utility. Despite its shortcomings, operators find they can quickly adapt and appropriate it for emergent needs. In a complex environment, we are better off doing a set of more general tasks very well, and enabling dynamic recombination of these general capabilities in new ways, than trying to anticipate, optimize, and over-specify all the particular capabilities that will be required.

> **Tenet 18**: Design for general utility; keep technology simple, robust, and flexible.

In the face of advanced automation such as machine to machine exchange of information, it is easy to temporarily lose sight of human roles, needed capabilities, and contributions. Yet machine-to-machine never exists in isolation; all information collection is ultimately human-directed (e.g., tasking selected sensors to collect intelligence of a particular type, at a particular time and location) and is ultimately intended for human consumption, so that it should more properly be labeled *human*-to-machine-to-machine-to-*human* (HMMH). People initiate, contribute to, propagate, and redirect machine-to-machine threads. The type and amount of contextual information or metadata that is required for *human* judgments is often different than that required for exchanges between *systems*. A key challenge of Human Systems Integration is therefore to design information sharing mechanisms and processes with an eye towards supporting the mixture of, and interplay between, both types of exchanges.

> **Tenet 19**: Facilitate the co-creation and co-evolution (between people and technology) of enabling environments.

In short, the enterprise exists to serve the needs of human goals and values. Rather than technology replacing people, people and technology will work together and complement each other in such "joint cognitive systems," where cognition is distributed across individuals, teams, and technology (Hutchins, 1995). And people will remain key players in such systems because of their creativity, expertise, and adaptability. Thus, the need to perform HSI in the systems of the future will only grow.

Enabling Technologies and Methodologies for Information Exploitation

Cognitive Engineering

Faced with the challenge of implementing HSI in ESE, the question is: How can Enterprise Systems Engineering make the best use of people and systems in large-scale distributed and dynamic enterprises? We believe one potential answer is to augment the practice of Systems Engineering with the methods of *Cognitive Engineering*.

Cognitive Engineering draws on a variety of disciplines, including Human Factors Engineering, Human-Computer Interaction, Decision Science, Cognitive Psychology, Computer Science, and other related fields. It has roots in Task Analysis, which identifies the key tasks or functions that are performed in a work domain and then systematically breaks each task into a series of lower-level tasks. Armed with such a task breakdown analysis, it is then possible to make engineering decisions about how to allocate functions between people and systems.

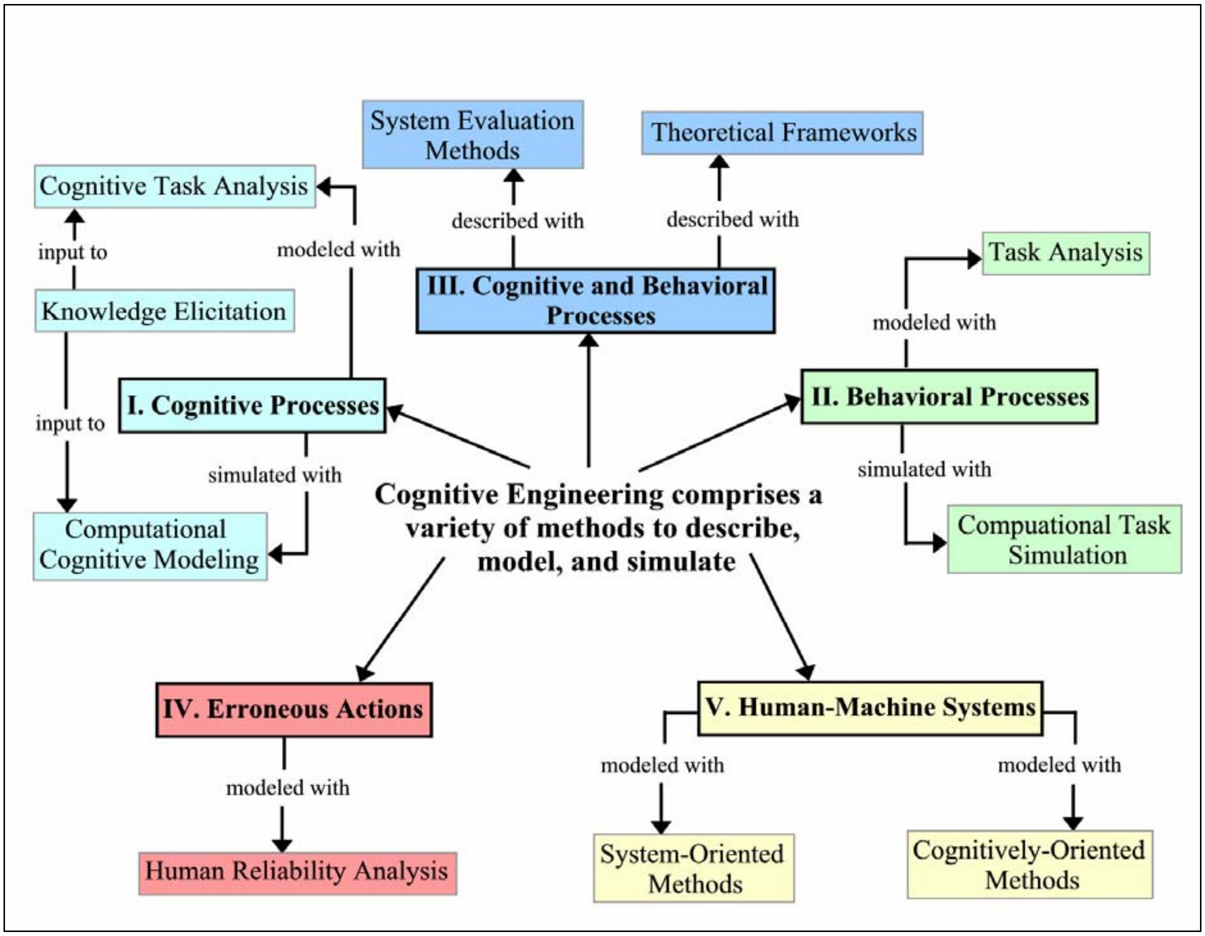

Figure 23: Classes of Cognitive Engineering methods

Here it is important to distinguish between *Behavioral* Task Analysis and *Cognitive* Task Analysis, since Cognitive Engineering is most concerned with the latter. Behavioral Task Analysis is concerned with actions (behavior) that can be directly observed, such as moving a dial or flipping a switch, and it is most often used to measure quantities like time-to-completion or total throughput in a given time. Cognitive Task Analysis moves beyond observable behavior to measure and model the mental activities (cognition) that drive observable behaviors, and it can be used to assess quantities like throughput as well as quality. For example, Cognitive Task Analysis can be used to assess the potential for human errors in information processing, and thereby serve as a basis for designing decision support systems.

The goal of Cognitive Engineering is to develop systems, training, and other products that support cognitive functions in decision-making, situation assessment, course-of-action selection, resource allocation and other information processing tasks. Some design questions addressed by Cognitive Engineering include: What information should be provided to system operators? How should the display be formatted so it is congruent with operator goals and decision-making objectives? How can tasks be effectively distributed across team members and system automation? How can systems support humans so that human-system performance is better than either systems or humans could achieve in isolation?

To answer these design questions, Cognitive Engineering methods are typically used to construct models that represent the cognitive demands of the domain. Figure 23 shows the various targets of analysis of Cognitive Engineering methods. These may include models of the decisions to be made in a domain and their interrelationships, the information required to support such decisions, cognitive strategies that are employed to process information and make decisions, as well as how decisions and tasks are distributed across agents in the domain, including people and automated support systems.

In order to advance the state of the art of Cognitive Engineering, we believe it is necessary to tie the analytical products of Cognitive Engineering more closely to enterprise systems engineering design challenges. Bonaceto lays the groundwork for integrating Cognitive Engineering into Systems Engineering in (Bonaceto, 2003). For further information on Cognitive Engineering, see (Bonaceto & Burns, 2006; Bonaceto & Burns, in press; Vicente, 1999), or visit the Mental Models MITRE Sponsored Research Cognitive Engineering web site, http://mentalmodels.mitre.org/cog_eng.

Intelligent Decision Support Systems and Automation

“Agile, effective decision making” is the crux of information exploitation. With the increased complexities of C2, such as the increased volume and rate of information, diversity of missions, compressed time-lines, and unpredictability of adversaries, it is imperative to provide operators with powerful and effective systems to support their decision making objectives. Unless the problem to solve is one that requires no flexibility in decision-making and a low probability of system failure, we believe fully automated decision support systems that provide operators with “optimal” solutions should not be the design goal. Rather, the goal (as stated in Tenet 4) should be to develop decision support systems that complement human decision makers to form an integrated human-machine team capable of solving difficult problems more effectively than either working individually.

In service of this goal, we present an approach to decision support system design called “structure mapping” (Burns & Bonaceto, 2006). The problem with most support systems is that they are not designed with adequate consideration of human cognitive and perceptual strengths. Structure mapping rectifies this shortcoming by constructing visualizations whose features directly map to the “structure” of the problem at hand. Such displays allow decision makers to reason about complicated situations with intuitive graphical representations. Geospatial maps are a simple example of structure mapping.

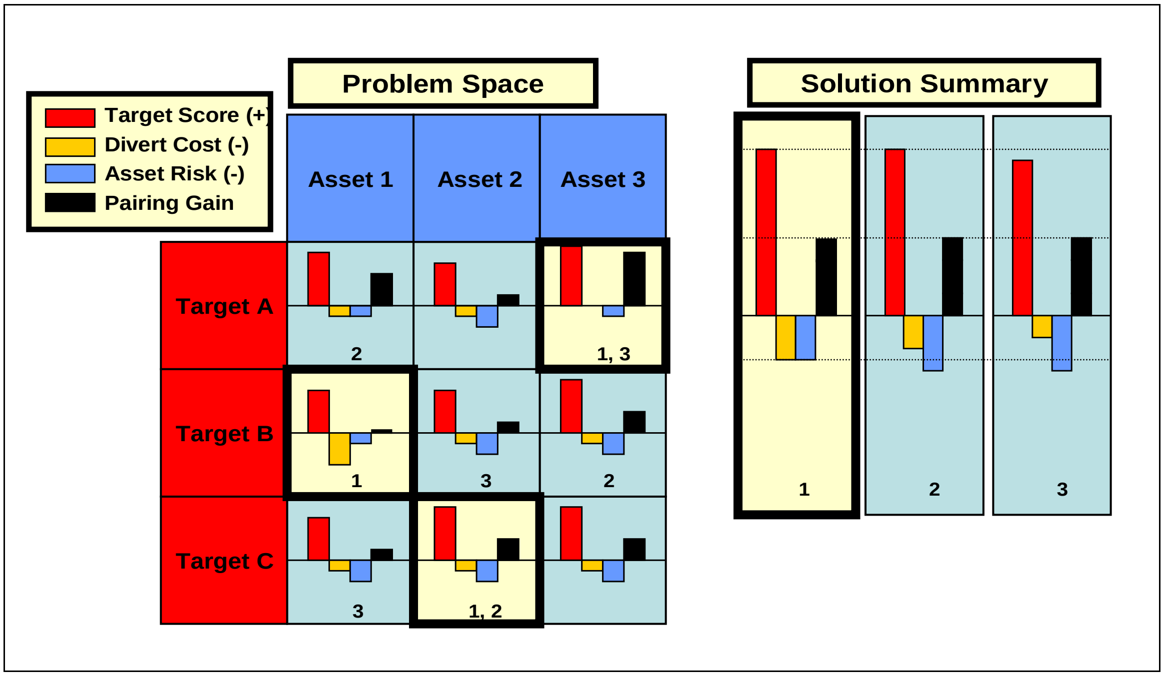

Figure 24: "Pairing Pictures" support system displays

However, many decisions in C2 require more robust representations than simple maps. One example is the problem of weapon-target pairing in time-sensitive targeting, an important resource allocation problem where operators must task a limited number of assets to destroy high value targets within a short window of time. Figure 24 above shows a display called "Pairing Pictures" to aid operators in weapon-target pairing that illustrates the principles of structure mapping. The basic structure of the weapon-target pairing problem is a matrix of assets paired with targets, which is depicted as the "Problem Space" on the left of Figure 24. The cells in the matrix represent the values of various weapon-target pairs, which is computed from a value function that sums the contributions of various factors including kill and loss probabilities, weighted by asset and target priorities The system design maps this structure to a matrix of boxes with color-coded bars that represent the different terms in the value function. This design arose from analysis of both the tasks to be performed in the domain, and the reasoning and representational strategies of human operators.

By designing displays that capture and represent the structure of the problem and mimic representations used by expert human operators, operators can rapidly perceive the problem space and select an appropriate course of action since less effort is spent on understanding the display. Thus, operators are able to devote their cognitive resources to solving the problem rather than figuring out how to use the tool. Moreover, if an operator's solution is at odds with the automatically computed solutions (shown in the "Solution Summary" in the right side of Figure 24), they can rapidly understand how the system came to its advice and rectify differences with their preference, which may be based on contextual factors that the system does not account for.

Tenet 20: Engender *appropriate* trust in and reliance on technology.

Information Exploitation Tenets and Design Principles

Information exploitation tenets and design principles have been highlighted and discussed above. Below, we briefly recap and summarize each tenet.

- **Tenet 1**: Provide feedback on surrounding context, as well as on performance. People provide the experience and perspective to detect cues indicating that seemingly valid and reliable system information no longer makes sense within the current context and thus violates an existing information pattern. They can initiate activities to determine whether the disconnect stems from the system information or algorithm itself, or is due to a perception of the environment that is no longer accurate. To support this "helmsman" role, systems must provide feedback on the external environment, in addition to feedback on progress towards specific ongoing tasks.
- **Tenet 2**: Design for "re-directability" of technological resources: The battlefield is complex and dynamic, and as situations and workload change, operators should be able to re-direct or constrain their technological resources. It is necessary for decision support systems to make clear their intent, assumptions, and operation so that operators can understand what the system is trying to do and decide whether or not what it is trying to do is congruent with what it should be doing.
- **Tenet 3**: Enable more *continuous* monitoring/characterization of the decision making environment. Complex and dynamic environments require ongoing human attention, supported by technologies, to detect cues that may herald a change in threat or necessary adjustment in information exploitation strategy.
- **Tenet 4**: Leverage and amplify (versus replace) human experience, insight, and adaptability. Humans are adaptable and creative decision making entities. The goal of technology should not be to replace humans, but rather to support their strengths and overcome their limitations. Performance of the joint human-technological system should exceed the performance of either working individually.
- **Tenet 5**: Link information generation, management, and exploitation efforts to enable dynamic extraction of the right information. The complexity of the battlefield environment requires that the critical function areas of information generation, management, and exploitation be well linked and integrated. That is, decision makers must have access to the current state of the battlefield to determine the impact of their decisions, a capability provided by information generation. They must also know

where to find such information and access it rapidly, which are capabilities provided by information management. Only then can they exploit that information and make timely decisions.

- **Tenet 6**: Facilitate *human understanding of* and *inputs into* determination of information pedigree, provenance, and trustworthiness. Decision makers contribute to the assessment of the source, pedigree, trustworthiness and reliability of information before they act on it. Thus, systems should provide contextual meta-data to facilitate this process. Since ambiguity is the rule rather than the exception in complex enterprises, determining information provenance is particularly important and challenging.

- **Tenet 7**: Value and facilitate information accessibility beyond its existence. Information exploitation must occur quickly enough to disrupt the enemy's decision cycle. Although the necessary information may exist, it is of no value unless it is identifiable as relevant to the decision at hand, and easily located and assessed by the decision makers in real time.

- **Tenet 8**: Design and introduce technologies with awareness of the actual work context, including interactions with other systems being used simultaneously. How decision makers actually go about their work is often radically different from the contents of documents such as Concepts of Operations (CONOPS) and Tactics, Techniques, and Procedures (TTPs). Operators adapt and utilize decision making strategies that often aren't articulated in such formal documents. Moreover, operators often rely on a multitude of systems and communication modalities. Thus, it is necessary to understand how operators actually perform their work to understand how a new system will impact operators' cognitive load and attention management as they interact with the new system in their work environment.

- **Tenet 9**: Design and introduce technologies to support information exploitation within the multi-modal communication environment. Operators often rely on multiple communication modalities (e.g., phones, radios, email, instant messaging, or face to face discussion). Multiple modalities may be needed to communicate with distributed team members and enable the necessary feedback and coordination for real-time team-level exploitation and response. Operators not only have to determine *what* information to focus their attention on and *with whom* to share it, but also must make countless secondary judgments about selecting a modality that will provide the desired response most effectively.

- **Tenet 10**: Automation should decrease, not increase, cognitive load in complex enterprises: A side-effect of many advanced automated systems is that operators are bored most of the time but overloaded during periods of high activity. Another side effect is that operators may either accept potentially incorrect automated solutions at face value or ignore automated solutions because the reasoning strategies of the system are hidden or not well understood by the operator. Moreover, if an automated solution doesn't gel with an operator's solution or preference, the operator may spend additional time and energy trying to rectify the systems' advice with his own preferences. Thus, the system has actually made the decision-making task more complex since the operator must decide wither to go with the system's answer or his own. Inserting automation into operator decision making tasks must be done with careful consideration of human-automation coordination, and automation should only be introduced when there is a specific need to do so.

- **Tenet 11**: Train as you Fight, Fight as you Train. The introduction of new technology changes the nature of people's decision making tasks and processes. New technology may introduce new types of errors and change the cognitive activities and strategies needed for effective performance. Thus, technology insertion must be an iterative process. We must develop prototypes, assess their utility in realistic scenarios, and refine and adapt them as we uncover additional demands that were not envisioned. This includes emphasizing team-oriented training and assessment for technologies that will be used in collaborative settings.

- **Tenet 12**: The "right" people in R4 is also dynamic; enable information exploitation across heterogeneous teams with changing membership. Information exploitation is a collaborative activity, requiring teams of typically dispersed individuals to conduct distributed decision making. Teams must achieve shared understanding and shared situational awareness in the face of different incentives, cultures, perspectives, and constraints. In highly complex environments characterized by emergent threats (such as Homeland Defense and Security scenarios), the composition and formation of the team itself becomes dynamic: the "right" people and corresponding resources are not fully known in advance, but rather must be assembled in real time.

- **Tenet 13**: Enable selective information sharing (to balance need for good judgments with risk of excessive distractions or cognitive overload). Though it may be tempting to share all information as broadly as possible in a network-centric environment, this quickly overwhelms human decision makers. Information must be posted and/or pushed selectively and appropriately to the "right people" ad the "right time."

- **Tenet 14**: Value more understanding over more information. Technological advances make it ever easier to gather and disseminate information. But care must be taken to avoid gathering information "for information's sake," potentially making it harder to locate attend to, and combine the highly relevant pieces of information for improved understanding and more informed decision making.

- **Tenet 15**: Provide mechanisms to maintain awareness of others' activities, knowledge, and load ("team awareness") to enable effective coordination. Since most information exploitation is the result of collaboration among people with differing expertise, roles, and resources, they must maintain "team awareness" in addition to situational awareness in order to coordinate effectively and achieve shared understanding.

- **Tenet 16**: Provide both *systems* to enable social, trust-enhancing interpersonal communication and *processes* to guide their appropriate use. Establishing appropriate trust among decision making entities is crucial to ensure agile and effective information exploitation. Issues of trust pervade all elements of the information exploitation environment: trust must be established not only between humans and technology, such as decision support systems and information sources, but also between human team members. Lack of trust is a potential socio-cultural "show stopper" for effective exploitation and decision making. Collaborative information exploitation requires rich interpersonal communication for some issues, and technologies to enable these less obvious but equally important drivers of communication. Both the development and the *implementation* of these modalities (e.g., training, tactics, techniques, and procedures) must be designed with an awareness of when and how they can aid information exploitation.

- **Tenet 17**: Emphasize and assess the performance of the joint human-technological "cognitive functional system." One way to characterize the C2 Enterprise is as a distributed "cognitive functional system," where cognition in service of decision making objectives is distributed across individuals, teams, and technology. End-to-end performance of an information exploitation system cannot be assessed in isolation from the people who will use and adapt the system. Objective criteria must be established to gauge the effectiveness of a combination of people, process, and technology in meeting enterprise goals. And the performance of the combined human-machine cognitive functional system should be greater than the performance of either the humans or machines working in isolation.

- **Tenet 18**: Design for general utility; keep technology simple, robust, and flexible. The "right" information is dynamic and determined by the current situation. Thus, there is a need for support systems to adapt to changing conditions. Since designers cannot anticipate a. priori each possible scenario in dynamic and fluid military environments, people should be able to adapt processes and technology to meet the emergent needs of the battlefield.

- **Tenet 19**: Facilitate the co-creation and co-evolution (between people and technology) of enabling environments. In the face of advanced automation such as machine to machine exchange of information, it is easy to temporarily lose sight of human roles, needed capabilities, and contributions. Yet machine-to-machine never exists in isolation; all information collection is ultimately human-directed, so it should more properly be labeled *human*-to-machine-to-machine-to-*human*. The type and amount of contextual information or metadata that is required for *human* judgments is often different than that required for exchanges between *systems*. A key challenge is therefore to design information sharing mechanisms and processes with an eye towards supporting both types of exchanges.

- **Tenet 20**: Engender appropriate trust in and reliance on technology. Operators must be aware of the uncertainty present in the information used by intelligent decision support systems. Moreover, automation should allow operators to rapidly understand the reasons and results of automated solutions, understand and adjust system parameters and assumptions as conditions change, and visualize and explore problem spaces so that they can calibrate an appropriate level of trust in dynamic and uncertain environments.

Information Exploitation Use Cases

Below, we highlight a group of current and proposed research projects in the information exploitation arena.

Mental Models in Naturalistic Decision Making FY01-FY03, FY04-FY06 MITRE Sponsored Research (MSR) Project

The primary goal of this research project was to improve human-system performance in complex domains, including military command and control, intelligence analysis, and air traffic control. In service of this goal, the project adopted a blend of behavioral and decision science to understand "how" and "how" well people think, especially in tasks that require making diagnoses and decisions under uncertainty. The project utilized a Bayesian framework as a normative standard for identifying where people perform well and where they can use help from computerized support systems. To perform experiments on human judgment and decision making that are both scientifically rigorous and relevant to real-world problems, the project developed a series of "synthetic task environments" that simulate key cognitive challenges in complex domains. One such synthetic task environment is Pared-down Poker, which is a scaled-down version of poker that simulates key challenges of command and control decision making, including opponent modeling and resource allocation.

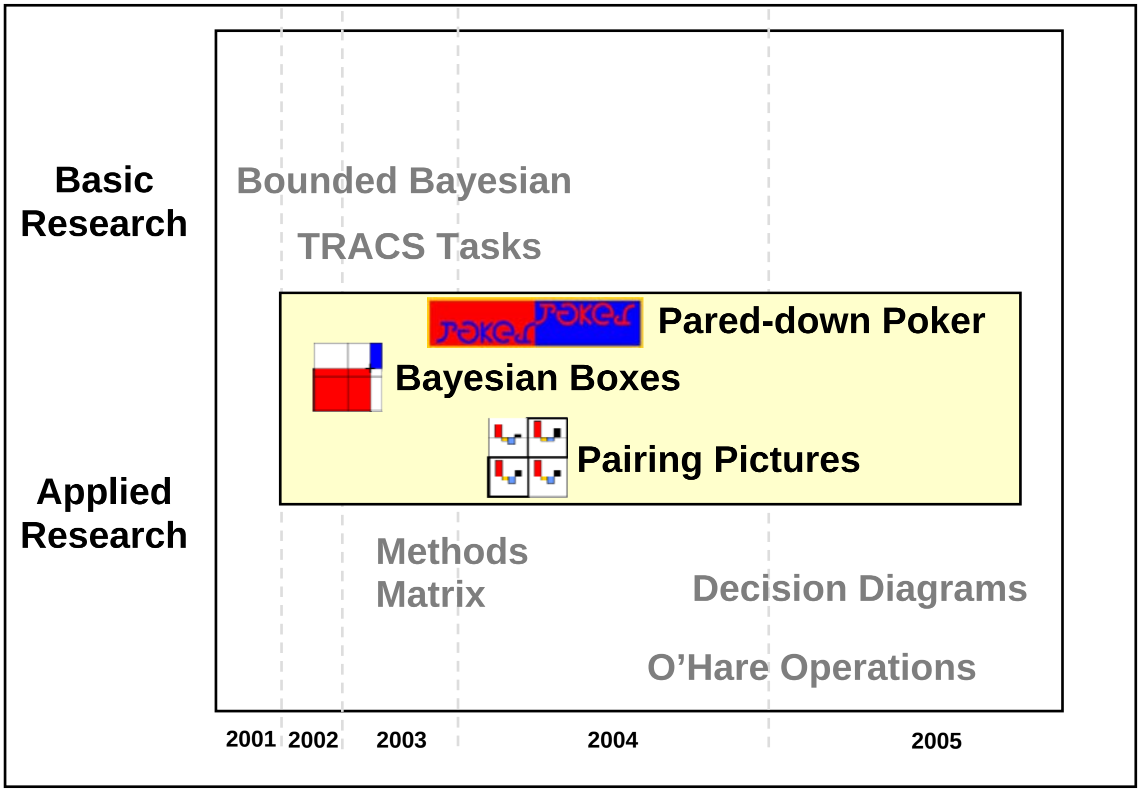

Figure 25: Research activities of the Mental Models in Naturalistic Decision Making MSR

As illustrated in Figure 25 above, the project's impacts and products run the gamut from basic to applied research. In the applied research arena, the project performed a decision analysis for the problem of Weapon Target Pairing in Time Critical Targeting that resulted in the development of a prototype decision support system ("Pairing Pictures" in Figure 25). It also participated in a collaborative effort with MITRE's CAASD to utilize the tools of Cognitive Engineering to characterize current operations and anticipate future operational challenges that may arise from runway or tower modifications at Chicago's O'Hare International Airport. The project has also performed an extensive survey of Cognitive Engineering methods (e.g. Cognitive Task Analysis, Cognitive Work Analysis) and has identified how those methods may best be applied to MITRE's systems engineering efforts ("Methods Matrix" in Figure 25). More information about the project is available at http://mentalmodels.mitre.org.

Improving Time-Sensitive Team Decision Making FY04 – FY05 Mission Oriented Investigation and Experimentation

The primary goals of this Air Force research project were to improve time-sensitive collaboration by making it quicker and more accurate in terms of decision outcomes, and with better processes leading up to the resulting human judgments and decisions. To improve time-sensitive collaboration, a critical objective was to identify human-system challenges, adaptations and emergent behaviors in context, in real time. Other objectives were to develop an explicit model of collaborative functions that must be enabled with better automation and processes, and to develop and employ an experimental environment to study team behaviors with additional rigor.

Key accomplishments of this project included the development of a three part methodology for studying collaboration in context and in real time; application of this methodology to several complex sponsor domains; documentation of operator adaptations and unexpected, emergent behaviors; development of a model of collaboration functions that must be supported by appropriate technology and processes; creation of a realistic experimental team environment for studying key collaborative processes with more control and rigor; developing tailored recommendations for several sponsor domains to improve automation and/or process; and preparing and delivering several research papers and conference presentations on our findings to facilitate knowledge transfer to sponsors, external organizations, and the research community.

Dynamic Diagrams in Asset Allocation

This Air Force research area addresses the increased amount of automation in C2 decision support systems brought about by NCOW. Many current automated systems are black boxes that shed little insight into the answers they provide. Thus, operators have little basis for knowing when to trust such systems as contexts change, and such systems do not leverage operators' adaptability and expertise. This research area aims to construct and evaluate an asset allocation support system (specifically, asset-target pairing for time-sensitive targeting) that will allow operators to understand, influence, and augment automated answers with their expertise. Its goals are to also identify key visualization and interaction techniques, appropriate levels of automation, and methodologies for developing automated support systems that will be applicable to a wide range of C2 asset allocation systems and automation problems.

5 Capabilities-Based Scenarios

Introduction

To demonstrate how the canonical functions of agile information generation, management, and exploitation come together to improve combat effectiveness in the C2 Enterprise, we describe an actual operational scenario called “Operation Anaconda.” Although ultimately successful, Anaconda was poorly executed and resulted in eight U.S. losses. We describe shortcomings in the planning and execution of Anaconda, and demonstrate how the capabilities enabled by the canonical enterprise functions that underpin our paradigm could be leveraged to improve performance in Anaconda and future operations.

Operation Anaconda

On March 1, 2002, an operation code-named “Anaconda” was launched against al Qaeda fighters hidden in the Shahi-Kot Valley and Arma Mountains southeast of Zormat in the steep mountainous terrain of southeastern Afghanistan. The operation involved about 2,000 soldiers comprised of conventional U.S. forces, Special Operating Forces, the 10th Mountain Division, the 101st Airborne Division, as well as Afghan forces and coalition forces from Australia, Canada, Denmark, France, Germany, and Norway. Although ultimately successful, Anaconda resulted in eight U.S. losses and dozens more wounded (“Army analyst blames Afghan battle failings on bad command set-up,” 2004).

In explanation of the casualties, Air Force, Navy and Marine Corps officials charged that the Army general responsible for planning the operation had failed to adequately include the other Services and relied on their hastily assembled support only as his battle plan began to fall apart (“Army analyst blames Afghan battle failings on bad command set-up,” 2004). When Army forces encountered unexpectedly fierce resistance from al Qaeda fighters, their commander issued an emergency call to the Air Force, Navy and Marine Corps air and naval fires and logistical assistance (“Left in dark for most Anaconda planning, Air Force opens new probe,” 2002). The response to the emergency call for fire was not as prompt or effective as anyone would have liked, contributing to the unnecessary losses and casualties. Figure 26 below highlights key criticisms of the conduct of the operation.

Army Major Mark Davis asserts that the Department of Defense failed to establish the command structures necessary to integrate the Services, and that the ambiguity in the command structure “created conditions that inadvertently excluded the Air Force from the planning of Anaconda” (Davis, 2004). A number of officers, however, disagree with Davis’ conclusions and point instead to such factors as insufficient planning and poor communication between leaders as more significant contributors to the outcome of the operation (“Army analyst blames Afghan battle failings on bad command set-up,” 2004).

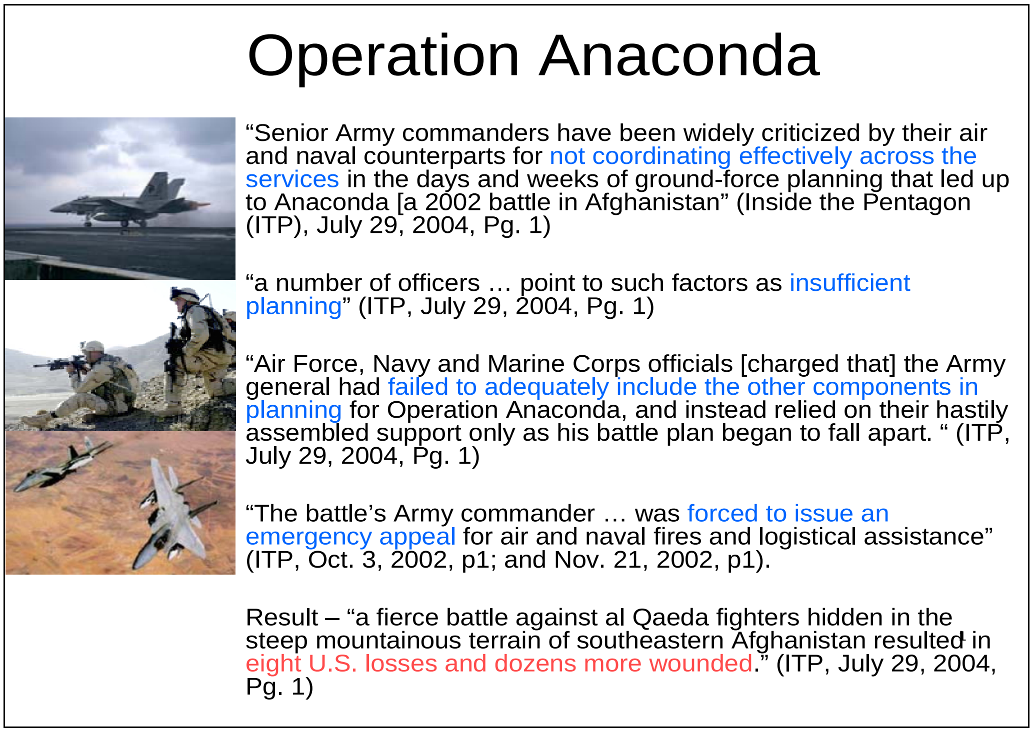

Figure 26: Key criticisms of the planning and execution of Operation Anaconda

Overall, the consensus is that the Services were not sufficiently coordinated during the planning phase, and that this lack of coordination contributed to both the need for an emergency call for fires and the difficulty in responding to it. Operation Anaconda posed significant challenges because it involved the use of multiple Joint and Coalition forces in a rapidly changing situation. Although challenging by historical standards, this kind of mission represents the future of warfare, and it is vital that we develop enterprise capabilities that ensure success in such military endeavors. In fact, the operation is often used as an example of the kinds of challenges that pervade planning Joint operations. It is therefore worthwhile to examine how a more effective combination of people, processes, and technology might have better supported the operation and resulted in fewer losses. Below, we examine how information exploitation, management, and generation--the three canonical function areas which underpin our Enterprise Systems Engineering paradigm--may be coordinated and applied to this operation and future conflicts.

Information Exploitation

An information exploitation tenet, discussed previously, is that technology exists to effectively support the processes and decision-making needs of the warfighter. Since finding and exploiting vast amounts of information requires teams of people in distributed environments, a key process in need of technological support and coordination is collaboration. In Operation Anaconda, for example, it is generally acknowledged that the

Army general did not adequately coordinate the integration of air assets from the Air Force and other Services into his battle plans. A collaboration technology that enabled joint operations in the planning phase would have remedied this situation by providing each component commander with a list of each operational activity and its current status. Without adequate procedures, training, and technologies in place, effective collaboration is unlikely to occur, as evidenced in the planning of Operation Anaconda. Thus, adequate collaborative processes and supporting technologies are needed to ensure that all decision-making entities remain informed of the existence and status of tasks to support operational objectives.

While human performance in tasks such as aircraft piloting and tank operation is well-understood, human performance in collaborative Command and Control (C2) decision-making processes are less researched and understood. This lack of research permits mistakes and oversights to seep into C2 collaborations at all levels. To remedy this situation, research in Human Factors, and Human System Integration is required in order to develop technologies that enable communication and knowledge-sharing at all echelons of command. If the component commanders involved in planning Anaconda had tools that provided insight into the existence and status of the various operations underway, they would have been more aware of the need for their involvement during the planning phase. Such early awareness creates a collaborative environment that fosters both buy-in and accountability. Early buy-in and accountability would have helped to ensure the availability of air assets and might well have obviated the need for the emergency call for assistance that occurred during the execution of the operation.

Another important aspect of information exploitation is the form and content of information presented to operators. Many systems have been developed without adequate consideration of operators' decision making needs; they simply display all of the information all of the time regardless of current operator goals (Boiney, 2005). Thus, there is a need for technologies that allow commanders to filter information content and selectively share relevant content with their team. Such technologies would also have applications in joint and coalition environments, permitting operators to share only information that is both relevant and approved. In Operation Anaconda, these technologies could have been used to help coordinate the joint and coalition forces during mission execution, possibly obviating the need to make an emergency call for air support.

Visualization technologies tailored to decision-making needs like those discussed above are clearly needed to eliminate information overload in network-centric environments and to decrease response times. Another enterprise-wide problem that hinders agility is that similar tasks are often supported by separate systems. For example, despite the similarity of resource allocation tasks like Weapon-Target Pairing (WTP), Intelligence Surveillance and Reconnaissance (ISR) tasking, and Close Air Support (CAS) mission planning, separate support technologies are being independently developed for each task. A better solution may be a more general resource allocation system for pairing assets to tasks. In addition to cost savings, such a system would enable agility since operators could be trained in the more general task of resource allocation, and thus be able to switch among resource allocation tasks in response to the operational demands of a dynamic conflict. Such a generic system could enable the AOC to alter its internal structure in response to environmental demands and remain agile.

Information Management

Additional difficulties were encountered during the execution phase of Operation Anaconda. Specifically, the other Services had difficulty responding to the emergency call made by the Army Commander. Although it is possible to point to shortfalls in the execution of the operation as the primary cause, a significant contributing factor is the planning process itself and the technologies that support it. Currently, Air Tasking Orders (ATOs) are developed for each 24 hour period. According to operators interviewed at the 9th Air Force Base, the ATO is most useful during the first three to four days of a conflict. Beyond the first three to four days, ATO changes become so frequent that the process becomes cumbersome and ineffective. A potential solution is to use well- scripted plans for the first 72 hours of a conflict and to then shift to a more dynamic allocation of resources in response to the ebb and flow of the battle. As an example, consider a flexible and dynamic resource allocation strategy where aircraft take-off in response to battlefield needs and are provided with a set of targets in flight. With such a strategy, there is minimal need to re-plan to perform Close Air Support (CAS), prosecute Time Sensitive Targets (TSTs), or prosecute Dynamic Targets, since there is no fully articulated plan to begin with. Target priorities are formulated based on commanders' intent, Rules of Engagement (ROE), available munitions, and mission dependencies. As a result, a target's priority combines data with pedigree from multiple levels. Once struck, targets would be added to the ISR deck for Battle Damage Assessment. In effect, ISR assets are dynamically tasked in the same manner as strike assets. This contrasts to the current process in which the ISR deck is configured during planning and does not necessarily work in concert with strike plans. Similarly, tanker refueling could also be scheduled dynamically across both the Mobility Air Force and Combat Air Force. Although the effectiveness of such dynamic scheduling processes would need to be borne out in simulations or exercises, we have illustrated new capabilities made possible by advances in information management.

As the line between system acquisition and operation continues to blur, creative and adaptable operators should be provided with technologies to build new capabilities on the fly. Currently, operators do indeed implement new capabilities in response to changing demands, typically with Microsoft products such as Excel and Visio. However, such ad hoc solutions are rarely documented or implemented in future command and control systems. Thus, there is a need to capture these operator-developed solutions and treat them as software specifications that drive the evolution of the Systems of Record. Particular attention should be paid to operator-developed solutions that address team decision making across the joint and coalition environment, since these are the most challenging requirements to capture in traditional software engineering requirements. Capturing and exploiting such operator adaptations for future use are essential in enabling a truly agile and robust C2 Enterprise.

There is also a need to capture and exploit data and information that passes through the AOC to allow warfighters to identify trends in enemy behavior and to automatically generate reports. Little data is warehoused in currently fielded systems, which inhibits commanders from obtaining accurate information about battlefield trends. It is common for commanders to make inquiries about the frequencies of events, such as requests for Close Air Support or diversions from planned targets to TSTs. Operators currently respond to such requests based on potentially flawed recollection and intuition. The lack of warehoused data also inhibits analyses of enemy intent. There is an enormous amount of information flowing through C2 systems that could be used to gain insight into enemy intent, identify trends, and improve our reactions and plans. But such opportunities are lost because the information enabling these insights is not presently captured. In the aftermath of Anaconda, timelines and events were reconstructed through operator interviews and written reports. Had more of the planning data and real-time information been warehoused, it would have been possible to construct such timelines and events more quickly and accurately to better facilitate analysis of the factors behind what went wrong. Furthermore, it is also likely that the existence of warehoused data would have permitted the analysis of more factors at a greater level of detail.

Another information management problem is that information representations tend to be specific to the processing needs of a single system, which inhibits the ability for a wider range of systems in the enterprise to make use of that information (see also Section 3). This detrimentally impacts the execution of joint and coalition endeavors such as Operation Anaconda. System designers must focus on the representational needs of the environment in which the system will be fielded, including unanticipated systems that might require the information. A potential solution to providing the kind of interoperability required in joint operations is the concept of "loose couplers," which would make it easier for each of the Services to evolve their systems independently while still maintaining the ability to exchange information (Electronic Systems Center, 2005, March). Had the joint and coalition forces engaged in Operation Anaconda been able to more easily exchange information during the execution phase, more responsive air support might have been possible.

In addition to the need for increased interoperability among the Services and joint forces, there is also a current trend towards greater interoperability among the Services and Special Operations Forces (SOF). In recent conflicts, for example, SOF have both identified and prosecuted TSTs. This close working relationship between SOF and other forces is a new development within the DoD, and has great potential to better deal with asymmetric threats. Previously, SOF worked largely independently of the other forces--a condition that occasionally caused significant problems for Blue Force Deconfliction. Aside from the increased use of Special Operations Forces, Army Forces like those engaged in Operation Anaconda often work in remote, bandwidth-limited environments. In order to support increased interoperability between the Services and SOF, we need to provide enterprise capabilities that support warfighters in such environments. In Anaconda, lines of communication between Army forces on the ground and supporting Air Force and Navy assets were circuitous and inefficient. Enterprise services that incorporate remote users could save lives by reducing timelines and increasing efficiency in joint missions. But the systems comprising the C2 Enterprise are heterogeneous in nature--a fact which requires accommodation when loosely coupling the multitude of subsystems. The U.S. Marine Corps intends to start exploiting smaller units with greater agility and autonomy that can combine into a larger force when more mass is required (McBrien, 2005). Incorporating such units into the C2 Enterprise will require a much greater emphasis on bandwidth-limited users.

Systems are currently designed with highly specified direct interfaces to their data and computational services. The use of highly-specified interfaces inhibits adaptation and agility by preventing systems from being combined in novel and unanticipated ways. Moreover, designers often specify the order of events or activities associated with a system, limiting the ability of operators to adapt their systems in the face of unanticipated events by reordering activities and changing decision-making processes. Systems need to be as flexible as possible by giving operators freedom to adapt their systems to changing contexts. As Enterprise Systems Engineers, we should encourage the design of systems with extensible and generic interfaces, and modules and modular decompositions should be used extensively to provide (re) combinable functionality. Such robust modules and modular decompositions will facilitate adaptation, evolution and emergence in decision-making environments.

Service Oriented Architectures and Enterprise Service Buses (ESBs) are a potential set of technologies that can address the problems recomposing modules in order to create new capabilities. In the Air Operations Center (AOC), for example, operators in the planning and ISR cells need to know which planned targets have been prosecuted. Although this information can be gleaned from network messages such as Tadil and SADL, it is not available in a form that makes it easily available to other users whose need for it was not anticipated in advance.

Another information management bottleneck is the tendency to force an artificial distinction between planning and execution. Such a distinction may be appropriate for large-scale force-on-force conflicts, but in the age of asymmetric warfare it limits agility. As an example, consider the problems that arise in performing Time-Sensitive Targeting within the constraints of the traditional planning cycle.

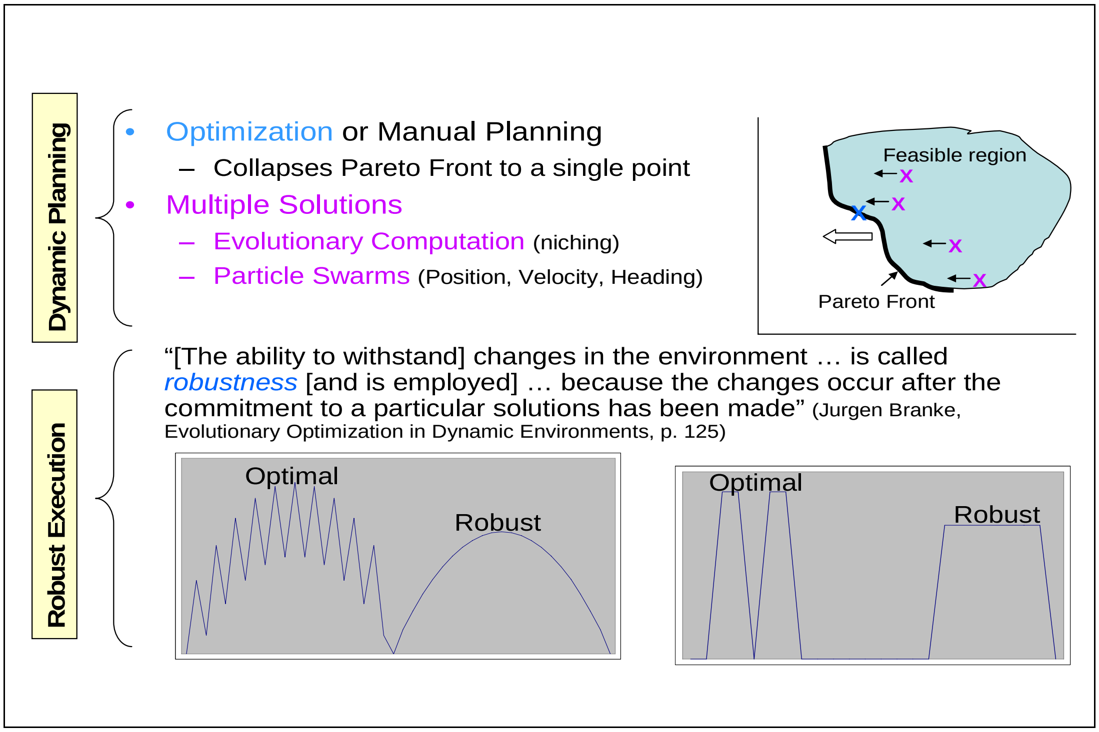

Figure 27: A characterization of dynamic planning and robust execution

In an attempt to remove the distinction between planning and execution, there are plans underway to alter the Air Operations Database (AODB) on a continuous basis. The current process employs an artificial distinction between planning and execution in which plans are highly-specified and changes are incorporated as updates to the plan. To be truly agile, there is a need to use flexible processes to find "good-enough" solutions to planning and execution problems. Optimization inhibits flexibility and adaptation. In the C2 Enterprise, deviations are the rule, not the exception. Thus, there is a need to trade optimization for flexibility and adaptation. It only makes sense to search for optimal solutions when there is ample time and the environment is relatively static. Figure 27 demonstrates the benefit of robust solutions in dynamic environments, where the efficacies of optimal solutions drop off sharply with minor perturbations in the environment.

Information Generation

One of the challenges of working in joint and coalition environments is the fact that there is no common representation of information pedigree across systems and Services. It is important that shortfalls in representations of information pedigree, accuracy, and latency are addressed. Although messages within a specific Service, such as the Air Force, often include measures of accuracy, there is no common representation for this information across systems within the Air Force, let alone across the various Services. This lack of standardization hinders the loose coupling of systems across different Services, hindering effective information management and exploitation. Furthermore, information representation standards also need to be developed for chat, UAV video and human intelligence reports. Because individual systems are part of the larger C2 Enterprise, it is imperative that issues relevant to enterprise-wide concerns, such as information standardization, be addressed.

Associating chat messages with track data and UAV video data is also problematic, and it is currently being investigated in an FY06 Air Force MOIE title "Collaborative Data Objects." Maintaining a correlation between a GMTI (Ground Moving Target Indicator) track and a UAV video track, for example, is unnecessarily difficult because the output from these various systems does not contain enough information to easily support correlation.

The FY05 Air Force projects entitled "Kaleidoscope: Multi-Sensor GMTI-VMTI Track Fusion and Visualization," explored ways to correlate color information from video streams with positional information obtained from video or other sources. Such an approach permits the aggregation of various types of information from a variety of sources, enabling more rapid discernment of the attributes of a track. Such an approach can be easily extended to integrate acoustic information as well.

In the C2 Enterprise, information can be used to support higher-level inferences. For example, information on the current status of a plan execution (e.g., the prosecution status of a target set) can be used to make inferences about the extent to which higher-level operational objectives are being met. Typically there are higher level combat objectives that are facilitated by a set of tactical objectives, which are in turn facilitated by a set of tactical missions, which may be facilitated by the destruction of individual targets at the lowest level of the hierarchy. This hierarchy can be traversed from the bottom up, so that information about the prosecution of specific targets is used to make inferences about the extent to which the higher-level combat objectives are being met. Figure 28 below shows an example objectives hierarchy.

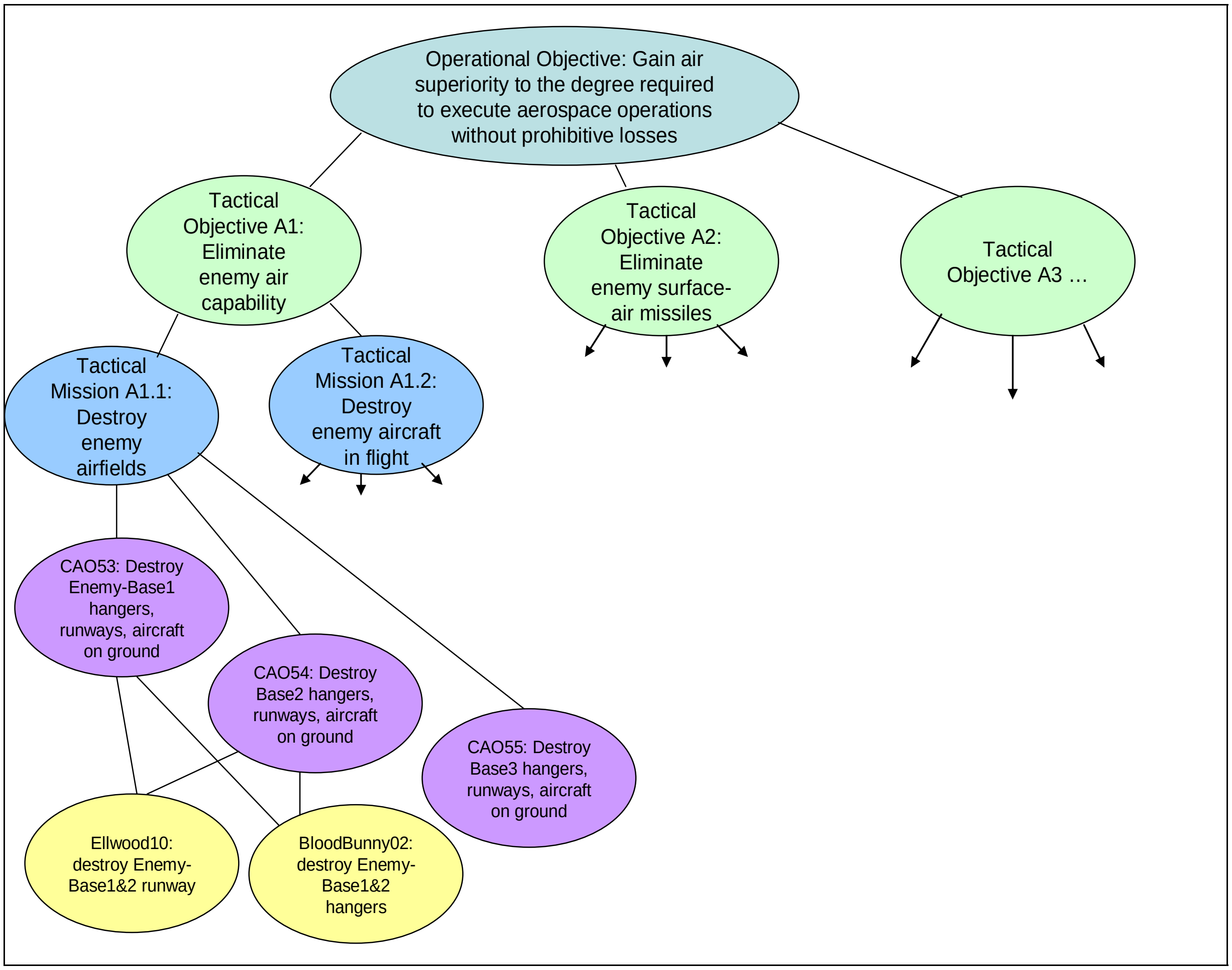

Figure 28: An operational objectives hierarchy

A more complex set of high-level inferences involves Effects Based Operations (EBO). Typically, missions are intended to achieve some desired effect, such as demoralizing enemy troops or forcing them to abandon certain locations. In EBO, the relationship between the specific tasks and the desired effects is less clear. It is possible, for example, to successfully complete all of the tasks without achieving the desired effects. Similarly, it is also possible to achieve the desired effects without having completed all the tasks designed to achieve that effect. Assessing the status of EBO is just as important as inferring the status of combat objectives based on the prosecution of individual targets, but is far more complicated to determine. Thus, it is an area for further research.

System Acquisition

One problem with the current systems acquisitions process is that in the typical spiral development cycle, the large number of requirements in each spiral has the effect of overfitting the system to the environment that existed when the system was designed, as opposed to the environment in which the system will be fielded upon completion. As the number of requirements increases, the system becomes increasingly sensitive to minor changes in the environment. Fewer requirements and increased iterations over shorter periods of time are one way to keep pace with a changing environment.

Another problem is that there are few established mechanisms for incorporating operational “lessons-learned” gleaned when systems are fielded into the evolution of the system or in the design of new systems. As a result, it is difficult to be agile in responding to emerging operator needs. The only goal should not be to have a system that is well-suited to a particular environment, but rather to have a system that is also able to adapt when problems occur or the environment changes. We need to evolve existing capabilities to accommodate change. One way to do this is to use such “lessons learned” to inform the evolution and design of both systems and processes. Enterprise Systems Engineering needs to implement traditions to add resistance to unnecessary change, while still recognizing that immediate action requires a response to severe problems. Rigid tradition and immediate action makes the process self-adjusting.

The acquisition community also needs to develop systems that are less specific and more general. Instead of building a tool that pairs weapons to targets and then modifying it for use in Combat Search and Rescue or Intelligence, Reconnaissance and Surveillance (ISR) cells, it would be better to build a tool that pairs assets to tasks generically. That way, operators trained on the use of the system could perform tasks for Time Sensitive Targeting cells, ISR cells, or CSAR cells. Not only would this save money by building a single, general purpose, tool but it would also make the AOC itself more agile by allowing operators to shift tasks based on the needs at the time. If the CSAR cell becomes very busy for a brief period of time, it would be possible to shift operators to that task until the backlog subsided.

6 References:

Ahmed, E., Elgazzar, A. S.,Hegazi, A. S. (2005). *On complex adaptive systems and terrorism*. Retrieved November 22, 2005 from the arXiv.org e-Print archive Web Site: http://arxiv.org/PS_cache/nlin/pdf/0501/0501032.pdf.

Alberts, D. S. (1996). *The unintended consequences of information age technologies*. National Defense University Press.

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series.

Army analyst blames Afghan battle failings on bad command set-up. (2004, July 29). *Inside the Pentagon*, *20(31)*. Retrieved November 16, 2005, from http://www.insidedefense.com/secure/defense_docnum.asp?f=defense_2002.ask&docnum=PENTAGON-20-31-1.

Axelrod, R. & Cohen, M. D. (2000). *Harnessing complexity: organizational implications of a scientific frontier*. New York: Basic Books.

Bieberstein, N., Bose, S., Walker, L, & Lynch, A. (2005). Impact of service oriented architecture on enterprise systems, organizational structures and individuals. *IBM Systems Journal*, *44(4)*. 691.

Berube, C. D. (2002). *Data fusion and the JDL model*. Unpublished briefing: The MITRE Corporation.

Boiney, L. (2005). *Team decision making in time-sensitive environments*. Paper presented at the 10th International Command and Control Research and Technology Symposium, McLean, VA. Retrieved December 8, 2005 from http://www.dodccrp.org/events/2005/10th/CD/papers/175.pdf.

Bonaceto, C. (2003). *A survey of cognitive engineering methods and systems engineering uses* (MITRE Product No. MP 03B0000061). Bedford, MA: The MITRE Corporation.

Bonaceto, C. & Burns, K. (2006). *Using cognitive engineering to improve systems engineering*. Manuscript submitted for presentation at the 2006 International Council on Systems Engineering Conference.

Bonaceto, C. & Burns, K. (in press). A survey of the methods and uses of cognitive engineering. . In R. Hoffman (Ed.), *Expertise out of context*. New Jersey: Lawrence Erlbaum Associates.

Burns, K. (in press). Dealing with probabilities: On improving inferences with Bayesian Boxes. In R. Hoffman (Ed.), *Expertise out of context*. New Jersey: Lawrence Erlbaum Associates.

Burns, K. & Bonaceto, C. (2006). *Structure mapping in visual displays for decision support*. Paper to be presented at the 2006 Command and Control Research and Technology Symposium.

Cabana, K. A.., Babich, A. M., Washburn, N. H. (n.d.). *Counterdrug surveillance and control systems: Using data mining technology to enhance detection and tracking of targets of interest*. Unpublished briefing: The MITRE Corporation.

Cabana, K. A. & Swarz, R. S. (2000). *Applying data mining technology to the CAFC2S work program*. Unpublished briefing: The MITRE Corporation.

Davis, M. G. (2004). *Operation Anaconda: Command and confusion in joint warfare*. Unpublished master's thesis, Air University School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama.

DeArmon, J. (2000). Identifying dominant air traffic flows in complex airspace. *The Edge: The MITRE Advanced Technology Newsletter, 4(2)*. Retrieved November 16, 2005, from http://www.mitre.org/news/the_edge/august_00/dearmon.html.

Electronic Systems Center. (2005, March). *Strategic technical plan v. 2*. Hanscom Air Force Base: Electronics Systems Center. Retrieved December 8, 2005 from https://enweb.mitre.org/tiles/content/references/documents/stp_guidance/stp/ESC_STP_v2.0_PR.pdf

Endsley, M. R. (2000). Theoretical underpinnings of situation awareness: A critical review. In M. R. Endsley & D. J. Garland (Eds.), *Situation awareness analysis and measurement*. (pp. 3-32). Mahwah, NJ: Lawrence Erlbaum Associates.

Hall, D. L. & Llinus, J. (2001). *Handbook of multisensor data fusion*. CRC Press.

Hanifen, T. C. (n.d.). *Joint vision 2020*. Unpublished briefing.

Hutchins, E. (1995). *Cognition in the wild*. Cambridge, MA: The MIT Press.

Klein, G. (1999). *Sources of power: How people make decisions*. Cambridge, MA: MIT Press.

Lamport, L. (1978). Time, clocks and the ordering of events in a distributed system. *Communications of the ACM*, *21(7)*.

Left in dark for most Anaconda planning, Air Force opens new probe. (2002, October 3). *Inside the Pentagon*, *18(40)*. Retrieved November 16, 2005 from http://www.insidedefense.com/secure/defense_docnum.asp?f=defense_2002.ask&docnum=PENTAGON-18-40-1.

Li, T. Y. & Yorke, J. A. (1975). Period three implies chaos. *American Mathematical Monthly*, *82*, 985-992.

Lin, H., Risch, T., & Katchanounov, T. (2002). Adaptive data mediation over XML data. *Journal of Applied System Studies (JASS), Special Issue on Web Information Systems Applications*, 3(2).

Malle, B. & Knobe, J. (2001). The distinction between desire and intention: A folk conceptual analysis. In B. F. Malle, L .J. Moses, & D. Baldwin (Eds.), *Intentions and intentionality: Foundations of social cognition.* Cambridge, MA: MIT Press.

Mathieu, J., Hwang, G., & Dunyak, J. (2006). *Transferring insights from complex biological systems to the exploitation of netted sensors in command and control enterprise*. Manuscript submitted for presentation at the 2006 Command and Control Research and Technology Symposium.

McBrien, S. (2005). *United States Marine Corps distributed operations architecture study*. Unpublished briefing: The MITRE Corporation. Retrieved November 16, 2005, from http://employeeshare.mitre.org/c/cbudde/transfer/Joint%20Lecture%20Series/JLS%2015%20Nov%2005%20Marine%20Corps%20Distributed%20Ops%20Enabled%20by%20C4ISR.ppt

McIntyre, G, A. (1998). *A comprehensive approach to sensor management and scheduling,* Doctoral thesis, George Mason University, Fairfax, VA. (DTIC No. ADA359079).

Mitchell, P. J., Cummings, M. L., & Sheridan, T. B. (2004). *Human supervisory control issues in network centric warfare* (Massachusetts Institute of Technology Humans and Automation Laboratory Research Report No. HAL2004-01). Retrieved December 10, 2005, from http://web.mit.edu/aeroastro/www/labs/halab/papers/HSC_NCW_report.pdf.

Mitleton-Kelly, E. (2003) *Complexity research approaches and methods: The LSE complexity group integrated methodology*. Retrieved November 10, 2005, from the London School of Economics, Complexity Research Programme Web site: http://www.lse.ac.uk/complexity.

Moffat, J. (2003). *Complexity theory and network centric warfare*. CCRP Publication Series.

Moody, J. & White, D. R. (2001). Social cohesion and embeddedness: A hierarchical conception of social groups. Manuscript submitted for publication to the *American Journal of Sociology*.

Orlikowski, W. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science, 11(4)*. 404-428.

Potts, D. (2003). Tomorrow's war. In Potts, D. (Ed.), *The big issue: Command and combat in the information age*. (pp. 9-28). CCRP Publication Series.

Sampada, C., Khusbu, S., Neha, D., Sanghamitra, M., Ajith, A., & Sugata, S. (2004). Adaptive neuro-fuzzy intrusion detection systems. *ITCC, (1)*. 70-74.

Scott, S. D. & Cummings, M. L. (2005). *Collaborative time sensitive targeting*. (Massachusetts Institute of Technology Humans and Automation Laboratory Research Report No. HAL2005-03).

Simpson, J. & Wiener, E. (Eds.). (1989). *The Oxford English dictionary, second edition*. Oxford University Press.

Szyperski, C. (2003). *Component software: Beyond object-oriented programming, 2nd Edition*. NY: ACM Press.

Thunholm, P. (2005). Planning under time pressure: An attempt toward a prescriptive model of military tactical decision making. In H. Montgomery, R. Lipshitz, & B. Brehmer (Eds.), *How professionals make decisions*. (pp 43-56). New Jersey: Lawrence Erlbaum Associates.

Tzitzikas, Y. & Meghini, C. (2003, August). Ostensive automatic schema mapping for taxonomy-based peer-to peer systems. Helsinki, Finland: CIA-2003.

Vicente, K. J. (1999). *Cognitive work analysis: Toward safe, productive, and healthy computer-based work*. Mahwah, NJ: Lawrence Erlbaum Associates.