Information Management Challenges on the Path to Net-Centric Operations

Tim Bass
Silk Road
bass@silkroad.com

Abstract: *Net-centricity, the notion of transforming large-scale intranets into capabilities-based, service-oriented architectures, exploits a new information management concept. Net-centricity implies that existing and future information systems within an enterprise will be engineered to publish product and/or service offerings within a strategic context that allows virtually all employees and applications to readily discover and use information. Therefore, the objective of net-centricity is to create the military equivalent notion of commercial electronic marketplaces for information that can adapt to challenges associated with the fog of war. Net-centric goals include breaking down organization stovepipes and facilitating dynamic information sharing and management practices by leveraging the principles of self-organization and market forces. With respect to large global organizations like the USAF and the DoD, this is a challenge that influences a wide range of social, technical and programmatic issues. In this paper we discuss information management in the net-centric environment. In the context of the discussion, we highlight a few of the challenges on the path to net-centric operations.*

Keywords: enterprise architecture, content staging, infomarts, information assurance, information economy, information management, information marketplace, information markets, net-centricity, net-centric information environment, service-oriented architectures, self-organization, shared spaces.

1 Introduction

Information networks, like the Internet, the DoD NIPRnet, and other physical networks have transformed the way organizations conduct operations, including the management of information within and across traditional organizational boundaries. These networks facilitate the rapid sharing of information. Producers and consumers of information are connected in a vast electronic grid which can be made available ubiquitously. From the airman on the flight line to coalition partners in other nations, the network forms an environment which participants are only a few clicks away from any other participant. In the context of communications and information exchange, every participant is a producer and a consumer in the *information economy*.

In this paper, we refer to the community of information producers, consumers and the infrastructures that facilitate the exchange for information as the information economy. The classical definition of economy or economic system is the system of production, distribution and consumption. Therefore, for purposes of this paper, an information economy is defined as the system of the production, distribution and consumption of information. The information economy is not constrained by finite boundaries and is indirectly governed by the cause-and-effect relationships of information supply-and-demand influenced by sets of regulatory or policy actions to compliment and stabilize the emerging marketplace.

The primary commodity on NIPRnet and the Internet is information, including text, still images, full motion video and audio. Net-centricity in the DoD, by its very nature is designed to benefit all producers and consumers of information. This, in turn, benefits the entire Department of Defense where information is viewed as a critical force-multiplier. For global organizations such as the USAF, this implies an *information marketplace*, i.e., an information economy of producers and consumers of information skilled in the rapid exploitation of net-centric technologies.

Net-centric information management is a new concept in the Department of Defense envisioned to orchestrate the vast number and wide variety of global DoD activities. It follows that net-centric information management is a key concept for USAF knowledge management and decision support. Digital information in the net-centric environment can easily be shared, disseminated, combined, linked and connected. Therefore, net-centric concepts and service-oriented architectures offer us both new possibilities and new challenges. Net-centric operations are less about centralized data management and are more about enabling flexibility, speed, dynamic organization of capabilities and services, in near real-time to achieve the desired effects and outcomes.

Net-centricity and the concepts of service-oriented architectures exploit new information management concepts. Information management, as used in this paper, implies a capabilities-based, service-oriented marketplace

for information. One of our critical military challenges is to use this agile, adaptive, information marketplace to open up hierarchical organizational boundaries and processes. In practice, this is a very complex challenge in large global organizations like the USAF and the DoD.

In this paper we examine key issues associated with net-centric information management. We begin by looking at the current state-of-the-practice in information management. We then explore the roadblocks to achieving dynamic event-driven real-time organization of capabilities and services to achieve military outcomes.

2 The State-of-the-Practice of IM

Traditional information management is dominated by the state-of-the-practice in enterprise architecture (EA) and can be summarized by three main activities: [i]

- Baseline the "as-is" architecture;
- Develop "to-be" structures and processes optimized for ROI; and,
- Align IT investments with the business/mission.

While there are numerous advantages to this structured approach, we must ask ourselves if it goes far enough in the net-centric environment. For example, the information environment and the underlying infrastructure are constantly changing. In recent years both the rate-of-change and the accelerating demands placed on the information environment far outpace the ability to create an enterprise view of the environment. Thus, ROI is inherently unpredictable.

Making matters even more challenging is the fact that the USAF must rapidly reorganize and respond to very different missions scenarios. The ability to rapidly adapt and respond to events when "the fight is on" and in "the fog of war" is a significant force-multiplier. It comes to no surprise that we are constantly reorganizing the information environment to meet the demands of ever changing missions—all while the information management environment is undergoing constant technological change. As if these challenges were not enough (!) consider the fact that no one airman nor senior executive has a crystal ball that provides a reliable view into future missions or business requirements. This uncertainty clouds our crystal ball. However, we are confident that the future is unpredictable and that change is both constant and inevitable.

These fundamental truths provide an important reminder for all of us. It is not sufficient to attempt to build information management architectures that align IT with "the mission." The military mission is dynamic-shaped by the ever-changing threat, our own success in operations, the political realities of life in a democratic society, and a host of other unpredictable forces. If we rely on the realignment of forces and operations within current guideposts associated with programs, platforms and systems we are highly likely to sub-optimize at best and, at the very least, create barriers (stove-pipes) to mission success. This state-of-the-practice in traditional information management and enterprise architecture does not address rapid adaptation to the constant change that characterizes the current global military and global military environment.

One school-of-thought is that the "as-is" activities of enterprise architecture have the unintended consequence of adversely consuming scarce organizational resources. Another school-of-thought has surmised that net-centric transformation in the DoD is based on leveraging the inherent power of the network to break down barriers to facilitate interchangeable IT assets, information sharing and effects-based operations. A key premise to this line of thinking is that traditional EA architectural models are useful but have the unintended consequence of contributing to compartmented thinking (functional sub-optimization), interoperability problems, and the proliferation of functionally elegant systems that fall short of contributing as much as they could to the desired military effects and outcome.

Net-centricity has been the flagship of the DoD vision to move the US military beyond organization, platform and system-centric state-of-practice toward a service-based approach characterized by speed of decisions, speed of organization, speed of action, precision of action, minimum losses and overwhelming victory. The next section discusses the construct of net-centricity in more detail.

3 Net-Centricity and IM

The term "net-centricity" in the DoD is used, almost synonymously, with the concept of "service-oriented architectures" (SOA). The DoD transformation is often generalized as a vision to leverage the concepts of a capabilities-based approach on both a strategic and tactical scale. Fig. 1 roughly illustrates a capabilities–based approach that implies existence of service-components and capabilities in a DoD SOA. Net-centricity builds upon the notion of leveraging the power of the network to facilitate the self-organization of event-driven capabilities in a rapidly changing mission and business environment.

As discussed in the previous section, capabilities are often bundled to form new capabilities, illustrated in Fig. 2. Fig. 2 also illustrates, at one level of abstraction, the family-of-systems (FoS) paradox. Existing capabilities

are often combined to create capabilities that have been historically referred to as family-of-system applications. There are many examples of FoS applications in the military, including GCSS, TBMCS, and GCCS.

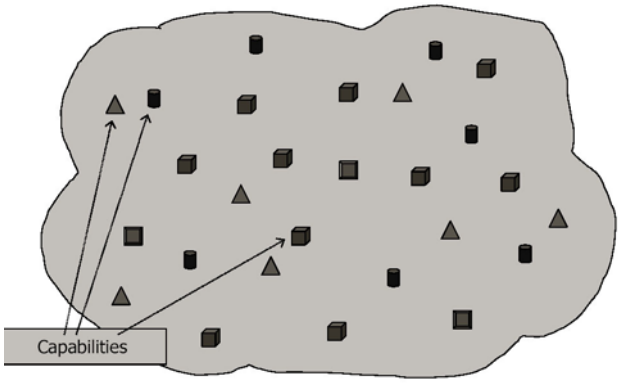

Fig. 1. Information Services as Capabilities[1]

Historically, these FoS applications, often consolidated under IT modernization initiatives or mission realignment objects, have proven to be expensive to build and operate. FoS applications also have exhibited the unintended effect of creating larger "stove-pipes" (barriers) from smaller "stove-pipes."

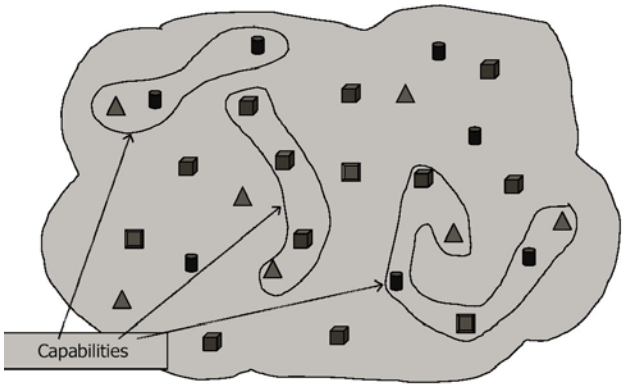

Fig. 2. Capabilities Create New Capabilities

Net-centricity and the information management transformation of the DoD has been geared toward moving away from FoS applications toward an SOA-based approach to information management. One metaphor that helps us to envision this transformation is the commercial concept of an "information market" based approach to information management in the military, illustrated in Fig. 3.

In the metaphor of Fig. 3, capabilities are organized into information markets. It is highly possible that the abstract information management processes of Fig. 3 may be self-organizing. There are some "information management rules" that govern the entry into the information marketplace; specifically the information producer must:

- Be connected to "the network";
- Publish the information products and services provided; and,
- Enable the widest possible access to all information products and services.

Connecting to the network is a relatively cost effective task in the world today, including the USAF and the DoD, because of the global standardization of the TCP/IP suite of Internet protocols. These standards-based protocols permit most information capabilities to seamlessly connect to a common infrastructure with minimal costs. In fact, there are very few technical barriers to entry into the information marketplace today because of advances in the Internet over the past ten years. Global connectively is now available in devices great and small, including airplane cockpits, cell phones, personal digital assistants, cameras, printers, electronic storage devices, cars, inventory control systems, desktop computing machines and more.

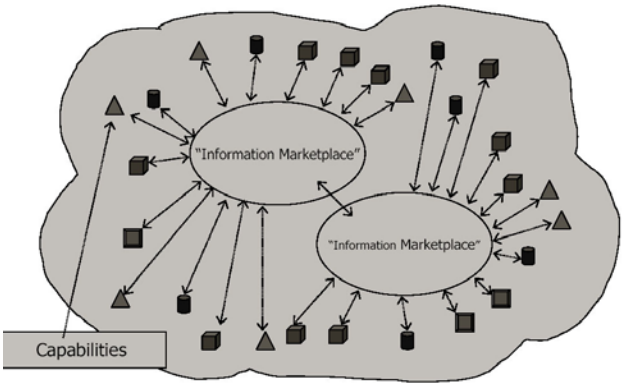

Fig. 3. Capabilities-Based Information Economy

One challenging aspect to information management may be for the information providers to view themselves as enterprise service-providers instead of program-centric system operators. Just as we build intelligence from sensors that can contribute useful information, and we build fighting capability from shooters that can contribute to the fight, we should build information enterprises from anyone who can contribute useful information.

Information service providers describe their information capabilities in terms of openly accessible network information services. The proliferation of Internets and

[1] Note: Need some capability and service labels on the objects in the cloud.-like airborne surveillance, HR, supply, fuel, moving target sensors, intel centers, operations centers, fighters, bombers, naval air, USMC air, etc

intranets into all facets of DoD and USAF operations insure a low cost of entry into the information marketplace. Another key challenge of net-centric information management is to insure that those artificial barriers to entry or access to the information environment are neither created nor sustained. Management must insure that an infrastructure exists that facilitates the dynamic, real-time organization and re-organization of information capabilities in the net-centric environment.

Net-centricity and net-centric enterprise services were originally envisioned as core infrastructure capabilities that were designed to lower the costs for producers and consumers of information to enter the information market place. For this vision to be realized, entry into and access to the information marketplace must be system and technology platform agnostic. When an information marketplace is created based on specific technology platforms or a vendor solution set, the goals and objectives of net-centricity are not realized because this type of process creates barriers. This is one of the unintended consequences of program and platform-centric information management practices.

Information management in the net-centric environment should be viewed from the perspective that information must be:

- Available as a network service;
- Accessible based on published standards; and,
- Accessible based on a need-to-share basis.

One of the inherent barriers to information management in the net-centric environment is the security implications of net-centricity in the emerging information marketplace. We briefly elaborate on this topic in the next section.

4 Net-Centricity, IM and IA

The metaphors and challenges on the path to net-centricity briefly introduced in the previous sections are small compared to the enormous information assurance challenges in the traditional need-to-know information management mindset. One of the reasons the need-to-know model fails is that the current and future information requirements of extremely large and diverse user populations are not predictable. Because the topic of information assurance is so important (and often very complex) it is best to discuss this topic in the context of the traditional domains of IT security, namely:

- Confidentiality;
- Authentication;
- Integrity;
- Non-Repudiation; and,
- Availability.

The reader familiar with IA concepts will readily recognize that the IA aspects of information management are more complex than the five security domains above when other factors such as accountability, multiple levels of access controls and risk management are factored into the information environment. Many have correctly pointed out that some of the greatest challenges to the goals of net-centricity are related to IA. The tension between the different schools-of-thought, for example the need-to-know versus the need-to-share, is acknowledged. Also, adding to the complexity (and economic costs) is the notion that the IA technologies that facilitate net-centricity tend to lag the non-IA related technologies.

These unavoidable IT security complexities in the net-centric environment often drive many net-centric design choices. Some would argue that the original business factors for establishing organizational portals were to reduce the integration costs of myriad data sources. One thought behind organization portals was to build "windows into the enterprise" that would, over time, permit single sign-on for access to organizational information assets. For example, one intended outcome of "the portal vision" was for users to authenticate their electronic identity (once) to the network using a common access card (for example) with embedded cryptographic credentials (PKI certificates). In portal architectures, the concept of cross-domain trust has been that digital authentication information would be proxied across the network, reducing security integration costs.

Another concept that has been envisioned to reduce the organizational IA costs in the net-centric environment is the notion of posting information to *shared spaces.* This concept encourages information producers to authenticate themselves to the network and to post information to shared spaces, such as a file system (like a web server) or an enterprise data warehouse. In this information assurance model, the costs of cybersecurity might be reduced because the shared space, or collateral space, can be the focal point of organizational capital expenditures.

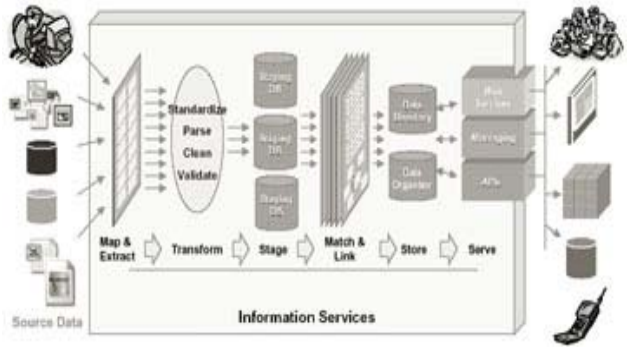

Fig. 4. The IM Environment (Courtesy of Xoriant)[2]

[2] For better clarity, redraw the Xoriant figure (in a future version).

Fig. 4, courtesy of Xoriant, illustrates the information management environment from the perspective of shared spaces. This model is quite powerful in the near term because it facilitates the concepts of the net-centric marketplace in a way that that is envisioned to make IA expenditures more cost effective. Fig. 4 also depicts the notion that structured, semi-structured and unstructured information is posted to shared spaces. There is no *a priori* barrier to entry into the information market based on a specific technology (such as XML) or platform (such as .NET or J2EE). Metadata may be manually or automatically created and this metadata is stored in metadata repositories, often called catalogs. The creation and access to metadata catalogs (such as the USAF equivalent to Google) are important cornerstones to a successful net-centric information management strategy.

Users of information in the net-centric environment, either human, intelligent software agents or computing machines locate information using different information search and retrieval techniques. Information search and retrieval techniques are variable, based, for example, on how the information will be used and who is the user. If the information is accessed via a web portal, the portal software should access myriad organizational shared spaces on the behalf of the user. Likewise, if the user is assessing information using a cell phone or a personal digital assistant, the software that supports cell phone or PDA access would also access shared spaces.

In a similar manner, when information fusion processing is orchestrated on the behalf of a user, the orchestration software could access the share spaces to obtain information from the required data sources. Performance requirements for insuring consistency between the shared space, for example a data warehouse and the originating data source, is based on information management policies. In this conceptual net-centric model, information is made available for a variety of technology platforms based on open technical standards.

From an IA perspective, users could authenticate to their network access point (web portal, for example). The network access point, by organizational policy, would have an established trust relationship with organizational shared spaces. The user roles, and other parameters associated with the identity of the user, are used for access to the information requested, for example. It is not necessary for the producer of information to have *a priori* knowledge about who are future individual consumers of the information asset.

Another challenge of this net-centric information management environment is that a taxonomy of organization roles should exist for a roles-based model to work correctly. This requirement leads to other organizational challenges such as the relationships between roles, rank and organization(s). The challenge of role-based access-control (RBAC) is also related to cryptographic administrative processes such as CAC and PKI.

Another challenging area to consider is the machine-to-machine synchronization of distributed information in the model of *infomarts* or *content staging,* illustrated in Fig. 5. This model implies that there is not one centralized shared space, but an entire network of shared spaces that disseminate information based on embedded information dissemination policies. This concept is congruent with the DoD vision of *"Power to the edge"* where information is staged close to the network consumer, greatly increasing the availability to the information consumer.

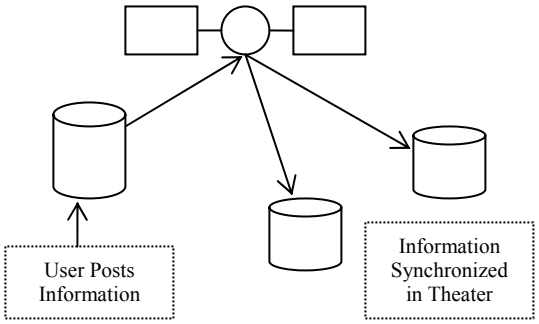

Fig. 5. Infomarts and Content Staging

Availability, confidentiality, integrity, authentication are examples of the IA challenges that must be addressed in the net-centric information management environment. When we view information management within the net-centric context of real-time self-organization of information capabilities in support of battlefield tactics, the challenges for all of us supporting USAF become even greater. We elaborate on these challenges in the next section.

5 Net-Centric IM in Fog of War

Clausewitz refers to the fog of war as its untheorizable turmoil, error, accidents, chance, the sheer, disorientation of combat terror.[ii] We will not attempt to cover the astute body of Clauswitzian knowledge and military discourse on the fog of war in this section. That is a topic best reserved for military experts and those who have served gallantly on the battlefield. Instead, the discussion in this section will narrowly focus on net-centricity and self-organization in the fog of war. I would like to thank Dr. Robert W. Zmud for his excellent paper, "*The Designing Organization in the Netcentric Economy* "[iii]. Dr. Zmud's insightful paper is the foundation for this sections discussion.

At one level of abstraction, net-centricity is about leveraging the power of the network (the Internet) to facilitate human relationships, linkages and interactions. These relationships are summarized by Dr. Zmud as *knowledge networks, trust networks,* and *cognition networks* in concert with managerial processes such as decision making processes, communication processes, control processes and improvisational processes influenced by organizational leadership. Together, these dynamic elements form the core of an organizational IT strategy.

As Dr. Zmud points out, net-centricity is the reliable instantaneous sharing of information assets and services both within and beyond an organization's traditional boundaries. Net-centricity facilitates the reliable instantaneous collection, aggregation, fusion, and customization of a broad array of data sources both within and across an organization's IT boundaries. Information filtering and fusion technologies continue to gain ground in the technological capabilities that attempt to mimic human intelligence. Net-centric information management, by its definition, accelerates and broadens organizational decision-making and decision-support.

Net-centric information management also facilitates the reliable real-time construction and reconstruction of the collective information contexts. It is within these information contexts that organizational action occurs. The commercial marketplace has accelerated deployment of architectures that almost guarantee the capability to rapidly interconnect, scale and componentize IT information assets. Therefore, it can be said that it is information, not the IT systems, platforms and programs, which accelerate and broaden an organization's business and mission transformation.

For global organizations, this implies the net-centric environment is transformed into the notion of an information marketplace. Dr. Zmud reminds us that the benefits of supply-driven competitive strategies are now possible because of the net-centric environment. Organizational stove-pipes can be turned into enterprise information service providers. One challenge lies in the organizational transformation toward a dynamic, self-organizing, virtual global organization. What appears clear to many is that the net-centric military of the future must be highly adaptable and self-organizing in peace time and in "the fog of war." The future net-centric Air Force, from an information management perspective, must be able to, in near real-time, dynamically reconfigure its information assets in response to unpredictable events. Organizations must be capable of dynamically re-organizing information assets in response to external events that are unpredictable and often chaotic.

Net-centricity is built upon webs of relationships, unconstrained by systems, platforms, functional domains, hierarchies or boundaries, ***to*** support rapid information flows and the concept of the virtual organization. Virtual organizations rely on IT to interconnect participants on a global and regional scale. No single department or group is charged with the responsibility to create and manage new knowledge and information; instead, every USAF member is viewed as a potential source of new knowledge. Knowledge creation is facilitated through self-organizing team-based structures and communities, unconstrained by platforms and system-centric progammatics. The communities within the context of the virtual organization provide a purposeful context for all Air Force members, uniformed military, civilians and contractors, to collaborate to reflect the strategic vision of senior Air Force and DoD executives.

In this context, information management in the age of net-centricity is founded on the principles of innovation, self-organization, and member ownership (accountability). While each autonomous team member, or virtual team, can act individually to meet specific mission objectives, collections of teams acting in concert can engage in more complex activities. It is precisely this combination of independence and interdependence that the military requires in order to operate and succeed in a world of uncertainty, disorientation, accidents and the terror of war.

The core enabling information assets of the net-centric organization are presumed to be knowledge, relationships, and capabilities. For the interested reader, Dr. Zmud's paper is an excellent starting point toward understanding knowledge, trusts and cognitive networks in the context net-centric information management. To summarize, net-centricity is envisioned to facilitate the dynamic real-time organization of information-based capabilities. This real-time organization and self-organization can be used to accelerate decision making, improve the quality of decisions, enable the achievement of the desired effects and outcomes—and do so in the chaos of the modern world and in the fog and terror of war.

Information management in the net-centric environment should facilitate individual innovation, dynamic self-organization and ad-hoc virtual teams. This environment implies a military marketplace of information-based capabilities. The strategic mission of information management in the net-centric environment becomes a mission to facilitate the dynamic real-time organization and re-organization of knowledge, trust and cognitive networks. *"Power to the Edge"* becomes a battle cry for *"Power to the Users"* and toward the real-time agility to self-organize as current military operations demand. Future events that drive how we will organize information assets are manifest in the chaos of the

battlefield, not in "as-is" and "to-be" architectural artifacts. Net-centricity is about capabilities; it is about what "could be" the nearly infinite arrangement of capabilities to meet emerging needs in the fast cycle connected society of today and in the life or death environment of combat.

6 Closing Remarks

It is possible to write page after page on the subject of information management in the net-centric environment. Perhaps the greatest challenge exists in each of our minds as we evolve our thinking beyond traditional systems, platforms, technologies and boundaries. This is an enormous challenge for all of us because systems engineering and platform acquisition activities are the dominate force in our information management activities. Organizations spend an enormous amount of time and resources building "as-is" and "to-be" architectures as they work exhaustively to align IT expenditures to missions that will, in all likelihood, end before the alignment is realized because the information environment and the underlying infrastructure are constantly changing.

One outcome for information management in the evolving net-centric environment is that USAF executives may make resource allocation (including funding) decisions for new systems based on their conformance to the principles of sharing information in an enterprise service-oriented architecture. The degree of compliance to these principles could be based on actual measurable information performance metrics. Examples of these compliance metrics include; how AF IT service providers function as an information service, how accessible and available are the information services they provide, and how accurate, reliable and trustworthy is the information they provide.

Another promising outcome of information management in the net-centric environment is that USAF executives may make resource allocation (sustainment) decisions based on measurable information usage data. The USAF could instrument the network to provide the capability to assess the value and performance of USAF information service providers. These promising outcomes of net-centricity may be further discussed in another paper.

We have briefly discussed information management challenges based on the net-centric notion of transforming large-scale intranets into capabilities-based, service-oriented architectures in an information economy. There are numerous exciting challenges on the path to operationalizing information management in the net-centric environment. The challenges are small compared to the potential benefits for the Air Force and the nation.

Acknowledgements

Lt. Gen. (Ret.) William Donahue, USAF, (Former AF Director of Communications and Information and Deputy AF-CIO) contributed to this paper providing revisions, collaboration and his thoughts on the subject.

Ms. Dawn Meyerriecks, (Former DISA CTO and now a Vice President with AOL, Time Warner), provided the opportunity to collaborate with some of DISA's thought leaders in the area of net-centricity, including Mr. Jim Pipher and Mr. Stan Davis.

I would like to close with a special note of appreciation for the inspirational leadership of Col. Anne Leary, AF-CIO, Plans and Policy Directorate (AF-CIO/P).

This work was partially supported by Silk Road contract GS-35F-0290K, Order Number T0503BM3283, HQ AF-CIO Network-Centric Systems Architecture, Strategy and Definition Task.

Biography

Tim Bass (bass@silkroad.com) is the President of Silk Road, a small business specializing in net-centric operational concepts, network systems engineering, architecture and security of distributed network applications. Silk Road has been providing independent, objective, Senior Subject Matter Expertise to the DoD for 12 years, including the United States Air Force (USAF), the Office of the Secretary of Defense (OSD/NII), and the Defense Information Systems Agency (DISA). He has advised the Department of Energy (DoE) and large, global multi-national financial organizations, for example, Chase Manhattan Bank, the Swiss Bank Corporation (SBC) and the *"Society for Worldwide Interbank Financial Telecommunication"* (SWIFT). Mr. Bass graduated B.S.E., Tulane University, School of Engineering, 1987 Magna Cum Laude, Electrical Engineering. Mr. Bass' work on Internet security and countermeasures for the DoD has been featured in Popular Science Magazine and Federal Computer Week. He recently completed two years of service as the Air Force representative to the Federal CIO Council, Architecture and Infrastructure Committee, Components and Governance Subcommittees. Mr. Bass is internationally recognized as a thought leader in numerous net-centric domains. His list of publications, detailed biography and company information is available at the Silk Road web site (www.silkroad.com).

References

[i] Whiteboard collaboration with USAF Lt. Gen. (Ret.) William Donahue, Vienna, VA, August 10, 2004.

[ii] Mann, Paul, *"The Nine Grounds of Intellectual Warfare," Department* of English, Pomona College, January, 1996.

[iii] Zmud, Robert W., *"The Designing Organization in the Netcentric Economy,"* Netcentricity Symposium, Decision and Information Technologies, R.H. Smith Business School, University of Maryland, March 30 and 31, 2001.

Public Release Approval

Review and approval of this paper by the Department of Defense for public release does not imply Department of Defense endorsement of factual accuracy or opinion.

This paper was cleared for public release by the Department of Defense on March 7, 2005, DD Form 1910 tracking number 05-S-0828**.**

