Enabling Technologies for Net-Centricity – Information on Demand

The Honorable John J. Grimes
Department of Defense Chief Information Officer

The focus of net-centric operations is to provide a more effective and efficient force that includes the warfighter, the intelligence community, and the business processes that support and enable the warfighters' success. The ability to access information, to share that information, and to collaborate with others is at the heart of net-centric operations. The ongoing transformation represents a fundamental change, a strategy that requires a cultural shift regarding how information and information technology is viewed and used.

We live in a new era. The relative predictability of the Cold War is gone. As the National Defense Strategy [1] states: *Uncertainty is the defining characteristic of today's strategic environment*. The strategy emphasizes that we will not know whom we will fight, nor when, nor where, nor how. As a military, and as a nation, we must confront uncertainty with agility. Our response to unpredictable, unanticipated, and unknown security challenges of today and tomorrow must be to ensure levels of agility never before considered and never before possible.

To support the warfighter in this changing threat environment, the Department of Defense (DoD) is transforming by leveraging the power of information. Information and the ability to access it, share it, and collaborate it with others is at the heart of net-centric operations. The recent Quadrennial Defense Review (QDR) [2], reinforced the importance of achieving net-centricity and called for 15 major information technology (IT) and command and control initiatives, and significantly increased efforts to ensure information can be trusted.

The focus of the net-centric approach and activities supports the DoD's transformation and the QDR goals: to provide a more effective and efficient force. That force is not only the warfighter, but it is also the intelligence community and the business processes that enable the warfighters' success. Regardless of time or place, the user must be able to say *I can get the information I need to perform my mission*.

Atop the particular activities and programs sits a fundamental change in philosophy: It is all about the data. To successfully implement a secure enterprise-level net-centric operations capability for the warfighter, we must move away from highly tailored programs that manipulate data and move to exposing the data in a timely fashion.

The ongoing transformation represents a fundamental change in approach – that is, a change in both what is being done and how it is being accomplished. However, underlying the new strategy is perhaps a far greater challenge. There must be a dramatic cultural shift with regard to how information is viewed and used.

Stewards, Not Owners

Today, information is typically stored in bins and silos that are walled off from anyone outside a particular community. There is not only a sense of data ownership, but also an enormous cultural reluctance to share with others outside a particular community. Additionally, existing systems cannot talk to each other without the benefit of time-consuming, highly tailored, costly, pre-engineered interfaces. The approach to information security is not much different. Everything is based on predetermined needs, despite the fact that in today's world it is not possible to anticipate what will be needed nor by whom.

There must be a complete overhaul in how information is considered. Instead of the parochial attitude that *information is power*, we must move to a culture that embraces and leverages the *power of information*. That rearrangement of words is not a subtlety but the reflection of a dramatically different culture and environment. The regulatory demands of *need to know* must be met. However, the culture must shift away from over-interpretation of the requirement and place greater emphasis on understanding who else would benefit by having the information accessible. The enterprise must make authorized information sharing a priority. The importance of *need to share* and, more importantly, *right to know* must be recognized. An authorized user, in essence, has the *right to know* information that is critical to doing his or her job. The ultimate objective is to connect people with information.

The DoD Data Strategy concentrates on realizing the principles that data must be visible, accessible, and understandable [3]. An authorized and authenticated user must be able to discover that data exists, pull it off the network, and use it. To do so requires *tagging* of all data with metadata and enterprise-wide registries to enable discovery by users. Communities of interest are forming across a wide variety of areas, including Maritime Domain Awareness, which has improved the ability to share information across the breadth of military, federal, state, local, and private organizations, increasing the security of our harbors and ports.

We must become stewards, not owners, of information.

Enterprise, Not Stovepipe

Today's data silos support a mentality in which information is, quite frankly, hidden and hoarded rather than visible and shared. Dealing with the unanticipated demands the latter. As the people, processes, and technology of the net-centric Global Information Grid (GIG) mature, the goal of sharing information must serve as the guiding vision. The challenge is to design, engineer, and create an information environment rather than focus on platforms and systems alone.

The approach, therefore, is to successfully introduce and continually evolve the GIG through enterprise-wide system engineering – not tailored stovepipes. This effort sets the path that the rest of the enterprise can easily follow by establishing enterprise-wide technical baselines, analysis capabilities, and compliance management. In short, emphasis must be placed on the whole enterprise and the foundation upon which it will support the full range of future users.

We must develop the net-centric GIG as an enterprise, not stovepipes.

Services, Not Systems

Today's world is focused on systems. That is, programs that retrieve and manipulate data are typically developed according to very specific and highly tailored requirements. Each organization or function tends to pursue its own needs. The result has been a bevy of systems that not only cannot communicate with each other but do not even use the same language. The proprietary applications currently in use are not open, not easily changed, and not transferable to other needs.

Services-Oriented Architecture (SOA) is the key to transformation in an age of shared information needs. Specifically, SOA supports an information environment built upon loosely coupled, reusable, standards-based services. It promotes data interoperability rather than application interoperability. SOA ensures providers can reuse what already exists – that is, pieces of applications and data rather than re-create them every time. Moreover, it allows new capabilities to be delivered more quickly. The practice of buying individual, highly tailored, proprietary systems must end. We must place a new focus on separating data from applications for use within and across the Enterprise Information Environment (EIE).

The second key to success is leveraging commercially managed services. The EIE will provide commonly available core services – that is, services commonly needed by a wide range of users. Services are required to access, manipulate, share, and, most importantly, collaborate data. They must be viewed as resources to manage rather than applications to own. Unnecessary duplication of services readily available in the marketplace must end. Buying *things* must be replaced with services purchased and billed based on usage. Simply put, the DoD will not develop, own, run, or install every service it might need. The Net-Centric Enterprise Services program under way at Defense Information Systems Agency (DISA) is key to how we are changing.

We must concentrate on services, not systems.

Portfolios, Not Programs

Finally, there is a fundamental change in the management and oversight of the many efforts involved in this transformation. It is a change that is understood conceptually and its importance is understood, but the actual implementation is still being sorted out. The 2006 QDR took steps to move us from threat-based acquisitions to a capability-based environment. In a world of unknown challenges and unanticipated needs and partners, focusing on capabilities is essential. The theory is on target, but the execution is tricky.

Traditionally, the acquisition environment has been viewed as a collection of programs and systems – that is, individual activities that lead to a specific product. Over time, the concept of systems of systems developed. Regardless of terminology, the emphasis was still oriented on delivering physical platforms or lines of code. There has been a tendency to create tidy packages that could more easily be managed – despite the fact that the relationship of the many packages to the warfighter's needs remained fundamentally unclear.

Net-centric operations will require bringing individual programs under umbrellas that represent actual and complete capabilities. The QDR initiated four Capability Portfolio Management (CPM) test cases. The CPMs not only pull related, integrated, and synergistic programs under a common management frame, but also consider whether or not there are duplications to mediate or legacy programs to cut. The process offers the ability to look at the whole rather than struggle to determine if there should be a connection between the parts.

In September of 2006, the Deputy Secretary of Defense (DepSecDef) signed a memo articulating the ultimate objective of the CPM test cases: *ensuring the ability to deliver a capability portfolio aligned with strategic intent*. In addition to that overall guidance on CPM, the leadership now regularly reviews progress through the DepSecDef's Advisory Working Group. The National Information Infrastructure/ Chief Information Officer (CIO) shares primary responsibility for the Joint Net-Centric Operations, and the Joint Command and Control test cases. Preliminary results from both have led to issue papers that are currently being reviewed by Program Analysis and Evaluation. The final two test cases, which the DoD also supports, are Joint Battlespace Awareness and Joint Logistics. These CPM test cases are consistent with the DoD policy on IT portfolio management. By focusing on capabilities needed, rather than programs funded, the needs of the warfighter are better met.

We must manage by portfolios, not programs.

Challenges Ahead

Much of what must be done is well understood, but many areas and needs have yet to be invented. Many challenges lie ahead.

Establishing an information sharing culture is critical; making it happen is equally critical. Cross-domain solutions are one of those challenges. Specifically, the movement of information across domains, both vertical and horizontal, must be addressed. Whether crossing organizational boundaries and moving information horizontally or maneuvering security levels and moving information vertically, the ability to leverage information throughout the national security community is essential.

Information Assurance (IA), another key area of focus in the QDR, is the basis for timely and trusted information. The threat is real. It is here, it is now, it is persistent, and it is *maturing*. Most importantly, we must change our approach. Security approaches must move from fences and patches that keep intruders out and toward data that is secure throughout its useful lifetime – secure from the start. IA is one of the most complex and important aspects of information sharing.

The *IA Component of the GIG Integrated Architecture* [4], originally released in late 2004, provides the strategy and the way ahead. It focuses on five goals covering protection and defense and creating the right workforce. It also includes a robust and growing identity management effort, including the issuance of more than 10 million common access cards (CAC) and a requirement from the Joint Task Force-Global Network Operations for CAC log-in with Public Key Infrastructure certificates.

There is yet another critical challenge – creating a Net-Enabled Command Capability (NECC). In addition to moving away from the current Global Command and Control System family of systems, this effort will also require a significant change in both mindset and approach. It will require moving from a static system and program-based acquisition environment to one that is dynamic and capabilities based. Also, it will change the current approach of *pushing* information to users, and instead will enable users to pull what they need and to contribute what they know. Instead of multiple architectures, it will be based on a single architecture. Perhaps most importantly, there will be a move from being platform specific and system driven, to platform independent and capable of dynamically meeting user needs.

As with many other aspects of the transformation, there are plenty of challenges for NECC in the months and years ahead. However, a program executive office has been established at DISA and an early 2006 Acquisition Decision Memorandum Exit Criteria was estab-

Coming Events

August 2-4
13th ISSAT (International Society of Science and Applied Technologies) International Conference on Reliability and Quality in Design
Seattle, WA
www.issatconferences.org/RQD2007page.htm

August 12-15
26th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2007)
Portland, OR
www.podc.org/podc2007

August 12-16
IWCMC (International Wireless Communications and Mobile Computing Conference) 2007
Honolulu, HI
http://dropzone.tamu.edu/~xizhang/IWCMC07/IWCMC07.htm

August 13-17
AGILE 2007 Conference
Washington, D.C.
www.agile2007.org

August 28-30
PerMIS '07
Performance Metrics for Intelligent Systems
Washington, D.C.
www.isd.mel.nist.gov/PerMIS_2007/index.htm

2008

Systems and Software Technology Conference
www.sstc-online.org

Coming Events: **Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: nicole.kentta@hill.af.mil.**

lished. Progress is indeed being made.

There are many other challenges that lie ahead. Most will require the innovative thinking that is best reflected by a sense of partnership with industry, academia, and technical associations. Success will be based on the ability to establish teams that are excited by the challenge, are ready to pursue new ideas, and can make things happen.

Summary

Information is a strategic asset. It is every bit as important as ships sailed, planes flown, and troops commanded, and, as an institution and a country, we must treat it as such.

Becoming net-centric is not about replacing the warfighter with technology. We will, for example, still need boots on the ground. Net-centric operations will allow humans to leverage information to better deal with unanticipated challenges, needs, partners, and circumstances.

Becoming net-centric means ensuring information is accessible throughout the enterprise from high-level headquarters and command centers to a soldier in a city tracking insurgents to a civilian at a depot in search of a new supplier. It centers on the knowledge that timely and trusted information can be shared with those who need it, whether alone or as a collaboration in groups.

Most importantly, becoming net-centric will allow the community to truly move to an information environment in which all participants, known and unanticipated, have confidence that they can get the information they need and they trust.

In the end, it comes down to a simple objective, one that is dear to our nation – saving lives. As we move into the future and deliver these capabilities to users across the enterprise, we must move as a team – a team that has a lot of challenging, yet very rewarding, work ahead. And I, for one, am looking forward to the journey.◆

References

1. DoD. The National Defense Strategy of the United States of America. Washington: DoD, 2005 <www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm>.
2. DoD. The Quadrennial Defense Review Report. Washington: DoD, 2006.
3. DoD. The Net-Centric Data Strategy. Washington: DoD, 2003.
4. DoD. "Information Assurance Component of the GIG Integrated Architecture, Ver. 1.0." Washington: DoD, 2004.

About the Author

The Honorable John J. Grimes was nominated by President Bush on June 17, 2005 and sworn in as the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO on November 14, 2005. He has extensive technical and policy experience in telecommunications, information systems, and the command and control fields. Grimes' public service includes the White House National Security Council Staff as Director for National Security Telecommunications Policy; Director of Defense Command, Control and Communications Programs; and Senior Director White House Situation Support Staff. He served as Deputy Assistant Secretary of Defense for Defense-wide Command, Control, and Communications and was the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures. As a member of the DoD senior executive service, Grimes held senior technical and staff positions with the National Communications System; Defense Communications Agency; and the U.S. Army Communications Command following his military service in the U.S. Air Force. Previously with Raytheon, he served as Vice President of Intelligence and Information Systems, Washington Operations. Grimes has served on four Defense Science Board Task Forces and was a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee. Grimes is a graduate of the University of Arizona, and has a master's degree from Shippensburg University in Pennsylvania. He is a graduate of the U.S. Army War College, Carlisle Barracks, Pennsylvania; the Federal Executive Institute, Charlottesville, Virginia; and Harvard University's National and International Security Policy program. He is the recipient of the American Institute of Aeronautics and Astronautics' Command, Control, Communications, and Intelligence award among other public, military and federal civil service awards, including two Presidential Rank awards.

6000 Defense Pentagon
Washington, D.C. 20301-6000