From the DoD CIO: The Net-Centric Information Enterprise

John G. Grimes
Networks and Information Integration
Department of Defense Chief Information Officer

Defense transformation hinges on the recognition that information is one of our greatest sources of power. Information can be leveraged to allow decision makers at all levels to make better decisions faster and act sooner. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it most is the heart of the capability needed to conduct Net-Centric Operations.

Returning to the Pentagon after more than a decade, one immediately senses being in the midst of the most significant military transformation in over 50 years. The Department of Defense (DoD) is at the pioneering edge of the ever-expanding information frontier. Today's effort will lead to a capability that empowers every user and every decision maker to access timely, accurate, and trusted data. It will allow sharing of information and collaboration throughout the DoD's Net-Centric Information Enterprise and around the globe. The policies, systems, procedures, talent, and culture being developed will ultimately result in timely decisions and decisive actions across the defense team. As both a force enabler and a force multiplier, it will result in greater operational effectiveness based on enhanced awareness and deeper knowledge. Most importantly, today's work is critical to ensuring the nation's security, both now and in the future. Being on the team is exciting and a source of great pride.

As the DoD Chief Information Officer (CIO), my first and foremost commitment is to lead the effort that will deliver the critical enabling capability required by the National Defense Strategy to conduct Net-Centric Operations (NCO): We will conduct NCO with compatible information and communications systems, usable data, and flexible operational constructs [1].

Our objective is simple: connect people with information. The required enabling capabilities will allow users to select applications, data sources, and services to create a customized capability to perform a desired task.

The ability to reach all the way to the tactical edge of our operations is essential – regardless of time or location. Daily activities, mid-term planning, and long-term objectives must directly support the realization of this essential capability. By operating as a team, NCO will become a reality.

The Context for NCO

Less than two years into the new century the nation became painfully aware that early 21st century security challenges would be characterized by a single word: uncertainty. Uncertainty is the defining characteristic of today's strategic environment [1].

Our national security community must address unknown and asymmetric threats, a wide array of missions, unpredictable situations, and fast-paced operations. At the same time, the nation will face these challenges with partnerships and teams that cannot be anticipated and which will include other governments, business and industry, as well as additional non-governmental organizations. It will be impossible to predict what information will be needed, where it will be needed, who will need it, or when it must be accessed. More importantly, critical decisions will be made on ever-shorter time lines. And, the actions of a young soldier in the field can have strategic consequences felt around the world.

> *"Instead of pushing information out based on individually engineered and predetermined interfaces, net-centricity ensures a user at any level can both take what he needs and contribute what he knows."*

Prevailing, much less thriving, under these conditions will require unprecedented levels of flexibility, adaptability, creativity, and resiliency. We must *confront uncertainty with agility*. Creating a Net-Centric Information Enterprise is the path to agility. Users at all levels and in all situations can access the best information available, pool their knowledge, and make better decisions, faster. *I can get the information I need.*

Simply put, net-centric means people, processes, and technology working together to enable timely and trusted *access to* information, *sharing of* information, and *collaboration among* those who need it most.

Establishing *trust* is essential to creating the information environment of the future. Ensuring trust in the system (availability), trust in the information (assurability), and trust in the participants (identity) will be critical to success.

A Net-Centric Information Environment

Instead of *pushing information* out based on individually engineered and predetermined interfaces, net-centricity ensures that a user at any level can both *take what he needs* and *contribute what he knows*. Reaching that objective requires new methods of dealing with data – an information age approach.

The net-centric data strategy meets this challenge by focusing on *data* rather than on the proprietary applications and programs that manipulate it (the current focus). Users and applications post all data assets to *shared* space for use by others in the Net-Centric Information Enterprise, possessing an authenticated identity and an authorized access (role-based). Those at the source of the data will be required to make it easy to find and use. It must be *visible*, *accessible*, and *understandable*.

Key to the data strategy are the users who need information. Communities of interest (COI) are collaborative groups of users who must have a shared vocabulary

to exchange information. Data characteristics and content will be *tagged* in an agreed-to manner. The communities will range from pre-established groups with ongoing arrangements to unanticipated users and non-traditional partnerships that develop on an ad-hoc basis. Individual users will determine and display content based on their specific needs, user-defined operating pictures (UDOP) rather than in rigid or pre-determined formats.

Information assurance, the greatest Enterprise challenge, is the basis for *trust* – trust in the system's availability, the participants' identities, and the data's dependability and integrity. Today, firewalls and software patches attempt to keep intruders out and data safe. Tomorrow's assured information will require that the individual data be secured throughout its entire useful life span.

The Global Information Grid (GIG) exists to connect people with information. The GIG is the fundamental enabler for NCO. It collects, processes, stores, and manages the Enterprise data. The GIG is not just a technological backbone. It includes people, process, and technology.

The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, and managing information on demand to warfighters, defense policy makers, and support personnel. The information capabilities that comprise the GIG include transport, Web-based services, information assurance technologies, applications, data, and architectures and standards. It also includes the tools, techniques, and strategies for managing and operating the GIG (e.g., Network Operations). Operating the GIG enables *information on demand*.

Enterprise-wide system engineering (EWSE) function will provide the necessary guidance to ensure the successful introduction and continuing evolution of the GIG. Providing end-to-end interoperability and consistent performance is essential across the range of business, intelligence, and warfighting functions. The EWSE responsibilities include continuous oversight of the GIG's evolution, developing and maintaining the GIG technical baseline, establishing Enterprise-wide capabilities to support decision makers, implementing a program compliance management construct, and overseeing Enterprise-wide experiments. Creating a defense information Enterprise bears little resemblance to the platform-oriented programs of the past. Given the range of development responsibilities, diverse sets of potential users, and wide variety of needs, the path to success depends upon a holistic approach and an Enterprise-wide system engineering effort.

The DoD CIO

The DoD CIO provides the leadership to meet the net-centric vision and ultimately deliver the critical enabling capabilities required by the National Defense Strategy. *Delivering the power of information*, the DoD CIO vision will ultimately lead to an agile defense Enterprise empowered by access to, and sharing of, timely and trusted information. It is our mission to lead the information age transformation that will enhance the DoD's efficiency and effectiveness.

Transforming to a net-centric force requires fundamental changes in process, policy, and culture across the DoD (defense operations, intelligence functions, and business processes). As the CIO, three key objectives are essential to successfully enabling NCO.

> *"Developing the capabilities that will enhance today's operations and agility is crucial to those of tomorrow."*

First, *establish a true information age CIO*. Now is the time to establish a well-understood and institutionalized role for the DoD CIO. Specifically, the defense community must move out of the industrial age mentality that places computers, data, and their support in an administrative role. Instead, the institution must view information as a strategic asset. Information is the basis of knowledge and action. Timely, accurate, and trusted information lies at the heart of the capability to NCO. Developing the capabilities that will enhance today's operations and agility is critical to those of tomorrow.

Therefore, the CIO must be an inherent part of Enterprise-level policy and planning. It is the CIO's responsibility to ensure that the information necessary to operate the largest business in the world is always available when and where it is needed. The DoD CIO has the statutory authority to carry out his responsibilities. The current challenge is to translate those responsibilities into leadership across the Enterprise and transform to an information-centered environment.

Second, *tell a clear and compelling story of where the Enterprise is headed and why*. Unlike designing a tank or launching a satellite, transformation to NCO is traversing new ground. Today, the community stands at the brink of an era where networked capabilities will increase efficiency, enhance mission success, save lives, and potentially reduce force structure both at home and in theaters of operation. Information is a *force multiplier*. The implications are being felt today and even greater effects in the future can be anticipated.

The fundamental concept of net-centric warfare is very different from Cold War norms. Information can no longer be treated as a possession that is controlled by an owner. Stovepipe systems will not lead to agile information sharing. Information needs cannot be predetermined and they must support participation by unanticipated users. Today, the underlying approach and initiatives associated with net-centricity are both hard to explain and hard to understand. The entire community must do a better job of making sure that there is a common, clear, and consistent message. The message must establish both understanding of, and support for, the information environment that will enable successful operations in the future.

Third, *create a 21st century work force of information pioneers*. The DoD has embarked on the most significant change since the 1947 Key West Agreement restructured the Services. Transformation is not new. History reflects many examples of how new capabilities *enabled* operations previously impossible to imagine, much less conduct. The advent of the telegraph changed Civil War operations as did the radio 50 years later. Today, information networks are essential to enabling the agility needed to face uncertain and ever-changing challenges to our security.

However, this transformation will not occur if the *business as usual* mindset prevails. The DoD must have the requisite understanding and skills of an information age work force. More importantly, the entire Enterprise must excite, attract, and leverage the cutting-edge talent that it will take to reach the vision of NCO. This effort should be viewed as *the* most exciting and challenging work being done across both the public and private sectors. The excitement surrounding this transformation must draw in the very best and the very brightest and then keep them so engaged that they will not want to leave.

Coming Events

August 13-17
2006 AFITC Air Force Information Technology Conference
Montgomery, AL
https://ossg.gunter.af.mil/aq/AFITC/Default.aspx

August 14-17
ISHM 2006
2006 Integrated Systems Health Management Conference
Cincinnati, OH
www.usasymposium.com/ishm/default.htm

August 14-17
2006 Space and Missile Defense Conference and Exhibition
Huntsville, AL
www.smdconf.org

August 14-18
11th IEEE International Conference on Engineering of Complex Computer Systems ICECCS 2006
Stanford University, CA
www.iceccs.org

August 14-18
SICPP 2006
The 2006 International Conference on Parallel Processing
Columbus, OH
www.cse.ohio-state.edu/~icpp06

August 28-September 1
SecureComm 2006
Baltimore, MD
www.securecomm.org

April 16-19, 2007
2007 Systems and Software Technology Conference

www.sstc-online.org

Conclusion

Clearly, exciting challenges lie ahead. Success will rely on the ability to address Enterprise challenges as an integrated team. Ideas and capabilities from the private sector and academia are critical complements to efforts in the public sector. Collaboration, as in any undertaking, is key to success. Inspiring creative minds and innovative thinking must be Enterprise-wide. Therefore, the public-private partnership must continue to develop, evolve, and strengthen.

The technological change we have embarked upon will be significant, but the cultural shift may be even more challenging. The hallmark of the 21st century is uncertainty. Net-centricity is rooted in a simple principle: *confront uncertainty with agility*. To be agile, data can no longer be *owned*, it must be shared.

Timely and dependable information will be available across the Enterprise from higher level headquarters and command centers to a soldier tracking insurgents or a civilian in need of a new supplier. Ultimately, net-centricity means *power to the edge* – the ability to deliver the power of information across the entire Enterprise.◆

Reference

1. Department of Defense. The National Defense Strategy of the United States of America. Washington, D.C.: Mar. 2005 <www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm>.

About the Author

John G. Grimes is the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. Previously, 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. Grimes has held senior technical and staff positions with the National Communications System, Defense Communications Agency and the U.S. Army Communication's Command following his military service in the U.S. Air Force, and is the former Vice President of Intelligence and Information Systems of Raytheon Company. Grimes is a graduate of the U.S. Army War College, the Federal Executive Institute, and Harvard University's National and International Security Policy program, and is the recipient of two Presidential Rank awards.

6000 Defense Pentagon
Washington D.C. 20301-6000
Phone: (703) 695-0349
E-mail: john.grimes@osd.mil

Web Sites

Network Centric Warfare Department of Defense Report to Congress

www.dod.mil/nii/NCW

From the Department of Defense's (DoD's) Web site, the DoD's report to congress on the future of Network-Centric Warfare (NCW) is easily accessible. On this page, you can view a PDF or Word document of the report.

The Seven Deadly Sins of Network-Centric Warfare

www.nwc.navy.mil/WARDEPT/7deadl~1.htm

The Seven Deadly Sins of Network-Centric Warfare (NCW) can be found on the Naval War Colleges web site. This witty look at the potential problems and misconceptions of NCW offers great insight into the potential of creating NCW within naval forces and also points out looming mishaps. The following are the seven deadly sins of NCW: lust, sloth, avarice, pride, anger, envy, and gluttony.

Defense Information Systems Agency (DISA)

www.disa.mil/main/about/missman.html

DISA is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other Department of Defense components, under all conditions of peace and war. DISA is the provider of global net-centric solutions for the nation's warfighters and all those who support them.