Overview of the Department of Defense Net-Centric Data Strategy

Anthony J. Simon
DoD CIO/Information Management Directorate

Net-centricity is the realization of a networked environment that includes infrastructure, systems, processes, and people. Net-centricity enables net-centric operations, a completely different approach to warfighting, intelligence, and business functions.

The Department of Defense's (DoD's) Global Information Grid (GIG) provides the foundation for net-centricity. The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policy makers, and support personnel[1]. The information capabilities that comprise the GIG include transport, Web-based services, information assurance technologies, applications, data, architectures and standards, and the tools, techniques, and strategies for managing and operating the GIG (e.g., Network Operations [NetOps]). By securely interconnecting people and systems independent of time or location, we can achieve substantially improved military situational awareness, better access to information, and dramatically shortened decision cycles. Our warfighters are empowered to more effectively exploit information; more efficiently use resources; and create extended, collaborative communities to focus on the mission.

The approach to implementing the GIG uses communications, computation, information assurance, and Web technologies, but we also recognize that the cultural barriers against trust and data sharing must be addressed. Hence, the DoD is using a comprehensive, integrated approach to deliver the foundation for net-centricity. This approach combines the DoD Net-Centric Data Strategy[2], an information assurance (IA) strategy, and the implementation of communications, computing, and service layers that comprise the Enterprise Information Environment (EIE) of the GIG.

The core of the net-centric environment is the data that enables effective decisions. In this context, data implies all data assets such as system files, databases, documents, official electronic records, images, audio files, Web sites, and data access services. One of the goals is to populate the network with all data (intelligence, non-intelligence, raw, and processed) and change the paradigm from *process, exploit, and disseminate* to *post before processing*. All data is advertised and available for users and applications when and where they need it. In this environment, users and applications search for and pull data as needed. Alternatively, users receive alerts when data to which they have subscribed is updated or changed (i.e., publish-subscribe). Authorized users and applications have immediate access to data posted to the network without process, exploitation, and dissemination delays. Users and applications tag data assets with metadata, or data about data, to enable discovery of data. Users and applications post all data assets to *shared* space for use by others in the EIE. The environment shifts from private data to community of interest or EIE data as a result of increased data *sharing* in the net-centric environment.

Prior DoD approaches to data attempted to standardize and control data elements, definitions, and structures across the DoD, requiring consensus among and across all organizations. The approach intended to promote interoperability through standardization of data elements, minimize duplication of data elements across the DoD, and reduce the need for data element translation. The prior approach proved to be too cumbersome to implement across an enterprise as large and complex as the DoD.

The DoD's Net-Centric Data Strategy defines a new approach to data within the DoD. The strategy expands the focus to visibility (e.g., tagging) and accessibility (e.g., exposure services) of data rather than standardization. It recognizes the need for data to be usable for unanticipated users and applications, as well as known users. The strategy identifies approaches that will improve flexibility in data sharing, supporting interoperability between systems without requiring highly engineered, pre-defined, tightly coupled pair-wise interfaces between them. This flexibility will be essential in the *many-to-many* exchanges of a net-centric environment. While tightly coupled interfaces between systems will continue to exist (e.g., sensor-to-shooter systems that require real-time, direct communications to close the kill chain such as a weapons targeting system), the objective in a net-centric environment is to increase the potential for many other systems to leverage the same data without having to anticipate and engineer this use during the development cycle of the producer system.

For example, sensor-to-shooter systems can offer *exposure* services that work *behind the scenes* collecting real-time data, storing it, and providing access to other users (e.g., through Web services). Exposure services can be designed to have little or no effect on performance critical processes and still provide system data access to unanticipated users. In the dynamic environment that the DoD faces, one in which systems are continually being developed, deployed, migrated, and replaced, it is imperative that unanticipated interfaces can be accommodated quickly. It is also necessary that systems be designed to separate data from applications, and where practical, allow *loose coupling* between services that expose and exploit data.

This data vision, as codified in DoD Directive 8320.2[3], is predicated on several key elements that are critical to realizing a net-centric environment:

1. **Communities of Interest (COIs).** COIs are collaborative groups of users who exchange data in support of their shared mission and who must have a shared vocabulary to understand their data. COIs support users across the DoD by promoting data tagging, creating catalogs of metadata for their data, registering their metadata for others to use, and creating access services. Data of interest to a COI can be advertised only for use by the COI or across the EIE. COI catalogs, which describe the data assets that are available, are made visible and accessible for users and applications to search and pull data as needed. A guide for COIs to address the implementation of DoD 8320.2 is pending signature and will be available through the Defense Technical Information Center Web site and through the DoD Chief

Information Officer (CIO) public Web site. The DoD CIO public Web site[4] offers a variety of links to information to help DoD personnel become familiar with related topics such as COIs and implementation specifics.

2. **Metadata.** Data about data is important to achieve the data strategy goals of making data understandable and enabling interoperability. Discovery metadata that is compliant with the DoD Discovery Metadata Specification[5] provides a way for data to be found by DoD search capabilities. When COIs register their semantic and structural metadata in the DoD Metadata Registry, it can be used by others to support interoperability and provide a richer semantic understanding of the associated data. The DoD Metadata Registry site[5] is used by COIs to register their metadata agreements that allow others to understand the semantics and structures of their COI data. The DoD Metadata Registry site also contains guidance on implementing the visibility goal of 8320.2 including reference implementations for tagging.
3. **Core Enterprise Services.** Core Enterprise Services are a common set of services for the GIG that enable data sharing, searching, and retrieving. The planned set of core enterprise services includes discovery, collaboration, mediation, messaging, information assurance/security, storage, applications, user assistant, and enterprise services management. Each of these services provides core capabilities that enable warfighters and business users within the DoD to get access to the right information at the right time. In essence, the collection of these services is similar to those underlying the ubiquitous operation of the Internet. For example, at the most basic level, the discovery service provides the equivalent of Google to the Internet; messaging provides the equivalent of AOL's Instant Messaging; and information assurance/security provides the equivalent of Microsoft's Passport, a single sign-on to multiple Internet capabilities. In the DoD's case, these EIE services are based on commercial products and services, but configured to meet the response times required for our warfighter's mission critical needs and hardened through rigorous information assurance/security. By building the GIG on these common services, every warfighter and business user who knows how to navigate the Internet and use a Web browser will be able to exploit the GIG. More information about the net-centric enterprise services program being managed by Defense Information Systems Agency is provided at <http://www.nces.dod.mil/>.

DoD Directive 8320.2 requires that components begin implementing the policies in the data strategy, and it requires the DoD's governance processes (acquisition, capabilities identification, and planning and budgeting) be modified to promote data sharing. The FY2006-2011 Strategic Planning Guidance (classified) has required the components to begin planning for and resourcing activities to make data visible, accessible, and usable. The DoD CIO is providing implementation guidance for and working with components, COIs, and program managers to ensure that data sharing practices are understood and implemented. By working with COIs (e.g., COI forums and pilot programs), the DoD can share lessons learned and improve overall guidance for increasing net-centric data sharing.

As a result of the 2006 Quadrennial Defense Review, a Program Decision Memorandum was issued that directed the DoD CIO to provide a defense-wide report to the Deputy Secretary of Defense on progress and impediments to implementing the data strategy. The DoD CIO will be working with DoD components and the information technology portfolio managers defined in DoD Directive 8115.1[6] to highlight successes, capture best practices, and identify obstacles that have to be removed.

The National Defense Strategy, March 2005, requires that the DoD *will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.* The DoD Net-Centric Data Strategy is a critical element to net-centric operations. The data strategy is the cornerstone to ensuring that information can be found, accessed, and understood by those who need it. The DoD CIO will continue to work with the DoD components to implement this priority.

Notes

1. See Department of Defense Directive 8100.1. "Global Information Grid (GIG) Overarching Policy." Sept. 2002. <www.dtic.mil/whs/directives/corres/html/81001.htm>.
2. Department of Defense Net-Centric Data Strategy <www.dod.mil/nii/org/cio/doc/Net-Centric-Data Strategy-2003-05-092.pdf>.
3. See Department of Defense Directive 8320.2. Data Sharing in a Net-Centric Department of Defense. Dec. 2004 <www.dtic.mil/whs/directives/corres/html/83202.htm>.
4. Department of Defense Chief Information Officer <www.dod.mil/nii/coi/>.
5. Department of Defense Metadata Registry and Clearinghouse <https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr>.
6. See Department of Defense Directive 8115.1. Information Technology Portfolio Management. Oct. 2005. <www.dtic.mil/whs/directives/corres/html/811501.htm>.

About the Author

Anthony J. Simon led the development of the Department of Defense (DoD) Net-Centric Data Strategy, which has become a widely known and referenced document and is perhaps the best description of the envisioned future environment. He assists the DoD chief information officer in managing, directing, executing, overseeing, and implementing many facets of information management across the DoD. Simon is responsible for providing policy and guidance for the DoD's net-centric data sharing direction. He has nearly 20 years of information management experience and for the last 10 years, has served as a senior information technology specialist for the Office of the Secretary of Defense (Networks and Information Integration). Simon has also worked for the Defense Information Systems Agency and the Defense Intelligence Agency. He holds a Bachelor of Science degree from Virginia Tech in Management Science and a Master of Business Administration from Marymount University.

DoD CIO/ Information Management Directorate
1851 S Bell ST
STE 600
Arlington, VA 22202
Phone: (703) 602-1090
Fax: (703) 602-0830
E-mail: anthony.simon@osd.mil