Practical Challenges Facing Communities of Interest in the Net-Centric Department of Defense

C. L. Connors and Dr. M. A. Malloy
The MITRE Corporation

Abstract
The United States Department of Defense (DoD) – one of the world's largest heterogeneous and distributed enterprises – is transforming its information management and sharing approaches in accordance with a net-centric data strategy. DoD traditionally has organized data practices along well-defined trust boundaries, with sharing occurring on a "need-to-know" basis. New solutions are expected to promote a "need-to-share" paradigm that enables all information to be available to all appropriate consumers within the enterprise. DoD has mandated the transformation to occur through the efforts of "coalitions of the willing," better known as Communities of Interest (COIs). How is DoD progressing towards its vision and what challenges do COIs face? Although the experiential insights we offer here are viewed from a DoD perspective, these challenges are equally relevant for thoughtful consideration by any commercial enterprise embarking on a similar evolutionary journey.

1. Introduction

Suppose you have been providing information management support within a large enterprise that traditionally has organized itself along organizational boundaries, with data sharing occurring on a "need-to-know" basis via well-defined, pre-engineered interfaces. Further suppose you are now expected to develop a new solution that conducts operations on a "need-to-share" basis, aimed at enabling all information to be available to all organizations within the enterprise whether anticipated *a priori* or not. Now imagine the enterprise you support is the United States *Department of Defense (DoD)* – one of the largest, heterogeneous and distributed enterprises on the planet.

The information sharing challenges you face have suddenly become exponentially greater. And by the way, the DoD is unable to directly fund this innovation, but mandates it to occur anyway through the efforts of "coalitions of the willing," better known as *Communities of Interest (COIs).* Today, this concept has leapt from imagination to reality as the DoD has indeed mandated a migration to an information-sharing future built around a "net-centric" data strategy. How is DoD progressing towards its vision, where information management and sharing solutions must cut across long-standing organizational and trust boundaries? What challenges has this created for those who support the transformation?

2. Background

2.1. The Net-Centric Data Strategy

Traditionally, DoD has approached the problem of interoperability – the meaningful exchange of data – by establishing well-defined point-to-point interfaces. While practicable, this approach results in the so-called *N-squared problem*: if data are shared among N participants, then each of the N participants must define (N-1) point-to-point interfaces, resulting in N*(N-1) interfaces overall. In other words, the complexity of this approach is N-squared.

DoD coupled point-to-point solutions with a data administration program that attempted to standardize and control the elements of data, their definitions and structures across the entire enterprise. While sound in theory, in many cases it has proven impractical, if not impossible, to gain consensus across an organization with the scope and diversity of DoD. Changes pose additional challenges as DoD must continuously adapt to new operational arenas and capability needs.

In a December 2001 memorandum, [1] the DoD *Chief Information Officer (CIO)* announced a plan to develop an enterprise-level data strategy to advance the Department towards the goal of net-centric operations. The CIO subsequently published a *Net-Centric Data Strategy (NCDS)* in May 2003 [2] as the foundation for managing DoD's data in a net-centric manner.

Net-centricity is the realization of a networked environment for warfighting and business operations founded on DoD's notional *Global Information Grid (GiG).* The NCDS defines the GiG as 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 policymakers, and defense personnel…independent of time or location." Colloquially, net-centricity is

sometimes referred to as "Google for the Warfighter" since it subsumes the idea of a robust enterprise-wide discovery mechanism to enable DoD consumers at any echelon to find and retrieve whatever information they might need to support their respective processes.

2.2. Communities of Interest

The NCDS also defines its COI concept as follows: "A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges." DoD envisions COIs as the net-centric focal points for data organization and management, moving these responsibilities to the organizational level that best understands the information exchange requirements fulfilled by their products.

DoD COIs will support consumers across the enterprise by providing the means for data producers to publish assets into shared spaces so they are visible and accessible. This is achieved by creating metadata catalogs, taxonomies and semantic ontologies that describe and expose assets, making them understandable to both human consumers and automated systems including search engines. The objective of this approach is to increase the utility of DoD's data assets beyond the confining community boundaries or "stovepipes" of the past. By poising data assets for search and discovery, consumers will be able to pull whatever data they need on-the-fly, without having to pre-engineer the exchanges.

We also observe that a fundamental reason DoD has established COIs as a net-centric mechanism is to tackle head-on the problem of taking authoritative data away from those who think they "own" it and therefore have the right to its exclusive use. While an individual Service component may operate and be responsible for the platforms from which particular data are collected, ultimately the DoD owns the data, not any individual. To the maximum extent possible, the NCDS envisions that all DoD data will be made available for broader, appropriate uses.

2.3. Pathfinding COIs

Obviously, COIs will need to establish operating processes and procedures to support their activities as outlined in the NCDS. Various pathfinding and pilot efforts are underway to refine the COI construct and to clarify its appropriate roles in the migration to net-centricity. For example, the need to quickly locate and eliminate a terrorist who may be moving from safe house to safe house was a strong motivator for organizing one of the first pathfinding COIs: *Time-Sensitive Targeting (TST)*.

A premise of TST is that such operations take coordinated efforts among multiple diverse participants, including: intelligence agencies, military and civilian forces, surveillance platforms, and vehicles to deliver ordnance (e.g., bombs) to eliminate the target. Through cumbersome point-to-point interfaces, such missions can take hours, if not days, to coordinate. The Air Force-led TST COI stood up to focus on developing and making available across the DoD enterprise those interoperable data representations and services needed to reduce how long it takes to put weapons on such fleeting, opportunistic targets.

2.4. Focus of this paper

Through our professional activities, we have been involved in hands-on work with several pathfinding COIs for the past 18 months. During this time we have become aware of some key knowledge gaps that are impeding COI progress. The goal of this paper is not to create a list of complaints about COIs or the NCDS. Instead, from the perspective of 50 combined years experience developing information interoperability solutions in general, we wish to expose these COI challenges for thoughtful consideration by a wider community of colleagues and technologists, in addition to all those in DoD who ultimately will be impacted by them. We point out areas where remediation is being applied and suggest additional on-the-horizon challenges for which actionable course corrections might be needed soon.

3. Practical COI challenges

The following paragraphs discuss some key COI challenges that we characterize as "knowledge gaps."

3.1. Data as an essential COI enabler

DoD Directive 8320.2, *Data Sharing in a Net-Centric DoD*, [3] observes: "It is DoD policy that … [d]ata is an essential enabler of network-centric warfare … Data sharing concepts and practices shall be incorporated into education and awareness training and appropriate DoD processes." We find, however, that this concept of pervasive practical sharing has not yet extended to the COIs themselves.

DoD plans to stand up infrastructure to support its asset sharing, such as registries where metadata can be exposed, and shared spaces where information resources can be published in support of DoD operations. But COIs need to share more than metadata and information assets generated by their data producers and the programs of record under their purview. COIs also need the means to easily share "introspective information" about themselves: the processes, lessons learned, and ideas they are creating

as living organizational entities that are standing up, maturing, sustaining, disbanding where appropriate, and generally conducting their business.

The pathfinding COIs are impeded by the same kind of "stovepipes" they were conceived to mitigate. Most COI work is proceeding behind organizational firewalls, or it is posted on "by-invitation-only" web sites that get in the way of free-flowing discovery and sharing. (Try a "Google" on "Department of Defense Community of Interest" and see for yourself.) Consequently, little practical sharing of examples, success stories, failures and expedient practices is taking place among DoD COIs.

The good new is, a few helpful how-to niche products are appearing in draft form from the more mature communities. Examples include Joint Forces Command's "COI-in-a-Box," Assistant Secretary of Defense for Networks and Information Integration's "COI Toolkit," and the Air Force's "COI Primer." Such guides will help the resource-constrained start-up COIs bootstrap and accelerate their efforts as they benefit from those more mature COIs who have gone before them. An even better, long-term solution will be the establishment of an overarching, DoD knowledge-sharing venue (e.g., web marketplace) to provide "one-stop shopping" for all things COI.

3.2. Metadata management

Additional knowledge gaps that are impeding COI progress lie in the realm of metadata management. Some exposition is needed to appreciate these challenges. The DoD *Discovery Metadata Specification (DDMS)* [4] defines metadata elements to assist with the discovery of resources published in DoD's shared spaces. The DDMS describes a common set of descriptive metadata elements that are to be associated with each data asset that will be made visible to the DoD enterprise.

Descriptive labels called "tags" will be inserted into assets prior to posting them into shared spaces. Tagging is a "mark-up" approach that provides a way of exposing the syntax of structured or semi-structured content. If these tags are related to concepts in a data model or an ontology, they lend some additional meaning to the published assets, making them more widely understandable. Neither the DDMS nor DoD has directed the level of granularity at which assets should be tagged. Instead, DoD components and other authorities have been advised to use "good engineering judgement" to determine which data assets should be made visible and how detailed the insertion of metadata tags should be.

When an asset is posted to a shared space, a DDMS-compliant "metacard" (similar to a library index card) will be created and registered into a metadata catalog. Among other things, the metacard points to the physical location where the described asset may be retrieved. The catalogs in turn will be exposed to search engines that process queries expressed in terms of the DDMS elements. Humans and automated systems that perform searches will discover data assets that have been tagged and registered into catalogs. This concept of operations is illustrated in Figure 1.

Thus the data assets linked to the metacards are poised for discovery once the appropriate enterprise services are deployed. It should be noted that the elements specified in the DDMS are platform, language and implementation "agnostic." It is the intent of the NCDS that system designers and engineers should be free to decide how best to generate and store DDMS-compliant metacards.

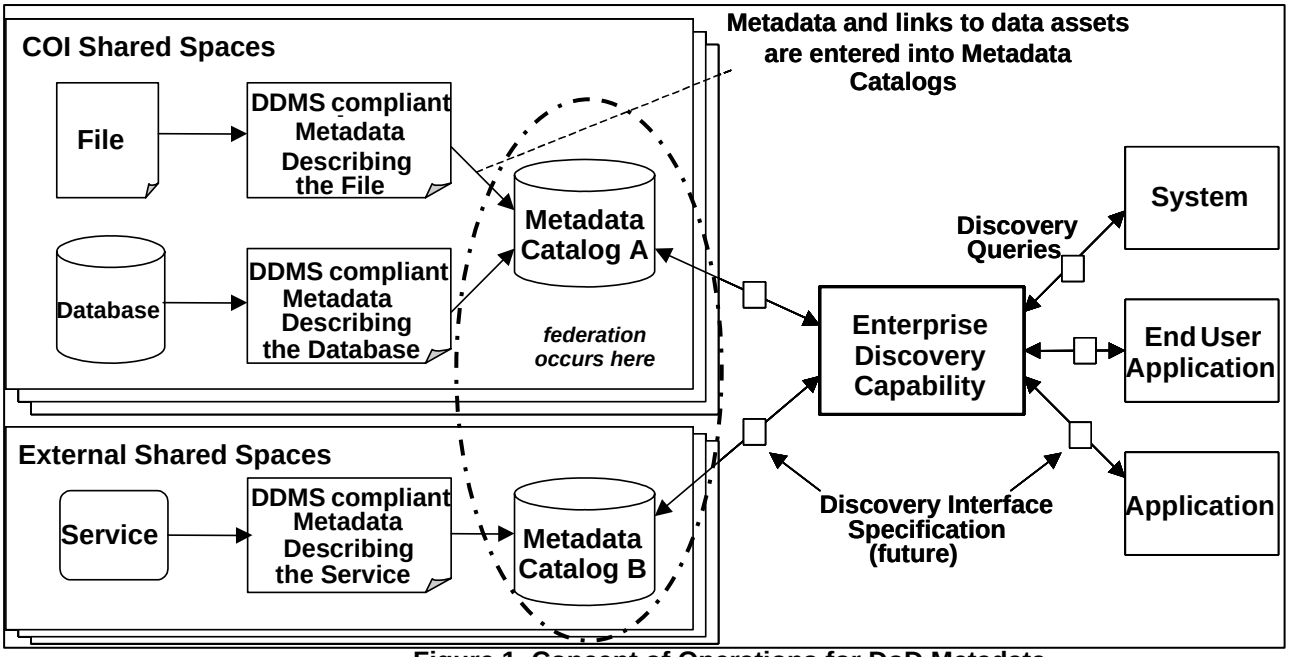

Figure 1. Concept of Operations for DoD Metadata

3.2.1. How much flexibility is too much? Because there are no overarching standards mandated for the metadata work, individual COIs have taken free rein to adopt whatever standards they choose, or none whatsoever. Vocabularies can be captured in word-processing documents, spreadsheets or even "mind map" diagrams. Data models and ontologies, developed formally or "mentally modeled" can be represented using any of a variety of graphics packages or more sophisticated tools such as ERwin. The potential for creating metadata products that will not be comparable across COIs is great. The foregoing description of the conceptual approach for enterprise discovery in DoD reveals how critical is the semantic layer for ensuring that meaningful linkages can be established from the ontologies that will be leveraged by search engines, to the tags within assets and the metacards that describe and locate those assets. If the semantic products of the COIs cannot be integrated harmoniously, this is a potential interoperability and discovery breaking point.

Similarly, there is a lack of guidance regarding the specific metadata products the COIs are expected to build. Most COIs we've worked with, despite considerable intellectual effort, have achieved only a rudimentary understanding of what is expected of them in terms of metadata, because only a high-level view has been disseminated by DoD. The relevance of the metadata artifacts and how they will interlock with the enterprise discovery services have not been articulated with sufficient clarity to focus COI efforts. For example, the flexibility in the DDMS specification offers too many confusing choices to COI implementors who are accustomed to receiving specific "what-to-do-and-how-to-do-it" guidance. In addition, little progress is being made in fleshing out the ontological layer. One reason why is the subject-matter expertise needed to help COIs make structural and semantic decisions is not often readily available to them.

Defense Information Systems Agency (DISA) has been proactively engaging with the more mature pathfinding COIs who are ready to start contributing to the metadata infrastructure. We are working with them to produce a concept of employment for the DDMS in the enterprise discovery context that will help clarify expedient implementation approaches and expected products for the COIs.

3.2.2. Single point of control or failure? The DoD *Metadata Registry (MDR)* [5] was established to serve as a hub for providing Department-wide visibility of and accessibility to structural and semantic metadata artifacts that are critical to the successful operation of net-centric capabilities. Once again looking to Directive 8320.2, [3] DoD states that "All metadata shall be discoverable, searchable, and retrievable … Data assets shall be made understandable by publishing associated semantic and structural metadata in a *federated* DoD metadata registry."

Our inspection of a recently drafted concept of operations for the currently deployed MDR revealed it does not incorporate a notion of registry federation. This is an implementation shortfall that must be repaired for the metadata infrastructure to function as intended. As illustrated in Figure 1, the NCDS vision intends that the metadata infrastructure be distributed, with communities establishing their own local metadata registries, federated for exposure through the MDR.

On the one hand, as presently implemented, requiring all communities to post metadata directly in the MDR might provide a centralized point of control and configuration management. Unfortunately, failure to federate the MDR is akin to the unsuccessful data administration approaches of the past; it is infeasible given the scope of the Department and will create a "single point of failure." Having so much metadata to inspect and interrelate in a non-federated structure will impede the efficiency of enterprise discovery and reuse. Federating the MDR is the intended approach; and it is the only reasonable, extensible approach as well.

Efforts are underway to turn this situation around. On behalf of our COI customers, we have been working to get clarification on the MDR concept of operations, to ensure there is a plan to accommodate federated community registries. In addition, we are seeing grassroots efforts focused on the federation aspect of the metadata registries and catalogs. The Air Force in particular has taken a lead in exploring the idea of community registries managed close to the assets they expose, and then federated to the central MDR, just as the DoD data-sharing Directive [3] originally intended.

3.3. Three complementary views

Although COIs were established with a data-centric focus, we have realized through our work with the pathfinding COIs that how best to satisfy information exchange requirements in the net-centric DoD cannot be assessed solely by considering data. Processes – re-cast as web-based services – and business rules are complementary views of the contexts in which the data and services are employed. All three have relevance, so the scope of COIs must include them all.

For the most part, pathfinding COIs have established a panel structure that segregates the data, service (process) and implementation practitioners from each other. This has created new organizational boundaries that impede COI members from synchronizing their efforts. COIs should take this lesson to heart and either avoid the panel structure in the future or establish internal procedures and communications threads that explicitly enable regular

cooperative interactions among the respective players. Business rules have received little attention to date within the net-centric migration, and consequently within COIs. This must change for a least two reasons.

3.3.1. Metadata tagging automation. The need to consistently tag published assets is a compelling reason why rule management must be addressed in DoD. The recent Air Force initiated Joint Automated Metadata Tagging Pathfinder [6] demonstrated that the quality of manual tagging is low and this approach is infeasible given the huge volume of DoD assets that need to be processed. Automated tagging methodologies are therefore essential to the success of the migration.

COIs can play a key role here by formally describing the business rules for how metacards associated with asset categories under their purview are populated with instance metadata. This poises the rules for importation into rule-aware applications that can algorithmically generate the metacards. Similar rule-based approaches can be pursued to help with the automated insertion of tags into into publish DoD assets.

3.3.2. Rules capture context. Another insertion point for rules technology is in the creation of agile, reusable services that support redefining the operational and business processes of the net-centric DoD. Rules that comprise the contexts in which data and services are employed presently are embedded in the legacy implementation code of programs of record, implicitly embodied in the structural interrelationships of legacy data exchange objects, written down as natural language in policy and procedures manuals, and hidden in the "grey matter" of human brains.

COIs are the logical place where mining and exposing DoD business rules can take place. The decoupling of rules from DoD core data and service components is essential to support reusing them in multiple mission-value chains. Instead of maintaining multiple tailored data processing aggregations – each tightly coupled for use in only one context – the rules-based approach is an extensible solution that allows different "rulesets" to be dynamically associated with generic data processing sequences (i.e., service orchestrations). Each ruleset adapts the generic sequence to the specifics of alternative operational or business needs.

The DoD net-centric metadata management concept must be extended to address rules management. The attendant roles and responsibilities for COIs must be thought through and then promulgated to them.

4. Other issues and challenges

We'd like to call out a few other issues and challenges COIs must deal with in the near future.

About 55 COIs have been established so far. Although DoD leaders expect to prioritize them and cull that number down, at present there are no processes in place for doing so. By what criteria will DoD identify areas of overlap in existing COIs so that one might subsume the other? How will the governance decision-makers recognize redundancy or other situations in which a proposed COI is not needed? Similarly, under what conditions is the work of a COI "done" so that it might be de-activated?

Questions like these point to the larger issue of metrics. DoD leaders have mentioned numerous intended uses for metrics to help answer questions about the progress of COIs in the emerging net-centric environment, such as service quality and user satisfaction, capability delivery and performance, return on investment, prioritization, and other matters yet to be determined. The metrics DoD collects for measuring the effects of the net-centric transformation must be constructed in ways that have relevance and meaning to the decision-makers. The methodologies for how to create meaningful metrics is still being discussed at the governance level. The outcome may put COIs under closer scrutiny and levy additional accountability responsibilities on them.

Secure, federated information sharing is a particular concern to us since several of our customers are engaged in sustaining long-lived interoperability agreements with coalition partners (i.e., NATO). Coalition interoperability to date has been conducted through a complex collection of bi- and multi-lateral agreements that require human intervention to negotiate and maintain them. Consequently, it's a brittle solution and change happens very slowly. Our coalition partners are on their own path to their own net-centric vision; they are making security attribution decisions for their assets to enable greater agility. Their decisions – like the recent incorporation of new security attribution tags in their metadata tagging design – will impact how DoD interacts with them in the future. COIs and the governance bodies that oversee them will be making similar security decisions for DoD assets. These decisions must be made with awareness and careful consideration of coalition solutions to ensure continued smooth coalition interoperations.

5. Conclusions and way-ahead

In this paper, we discussed essential elements of the NCDS and several practical challenges facing COIs as they assist DoD in the migration to net-centric operations. Knowledge gaps are impeding COI pogress in the following areas: free-flowing sharing of introspective information to learn from one another; understanding their expected engagement and products relevant to metadata management; and incorporating the complementary views of data, services and business rules in their analytic

activities. We also mentioned a few other COI challenges we see on the horizon.

The experiential insights we shared were offered from a DoD perspective, as the Department transforms to information management and sharing solutions that cut across long-standing organizational and trust boundaries. However, we believe the challenges faced by DoD COI practitioners are highly relevant to their counterparts in any large, heterogeneous commercial enterprise embarking on a similar evolutionary journey.

To accelerate the progress of COIs or other entities stood up for similar purposes, the enterprise must concurrently stand up the information infrastructure that will enable them to share examples, best practices and lessons-learned easily with one another. In other words, consistent with what the enterprise preaches, COIs must be empowered to practice the widest appropriate exposure of their products, processes and experiences, making them available for reuse as models by others with similar goals and purposes.

We also pointed out how critical it is for the enterprise to drive down the details of the migration beyond the visionary level so that practitioners understand enough about what is expected of them to make meaningful, progressive contributions. Primers and toolkits are effective niche products that bootstrap the efforts of nascent COIs and provide a feedback mechanism for more mature COIs to help the emerging ones along. A COI knowledge-sharing marketplace on the web would be even better.

The enterprise must be ready to embrace not only technology innovation, but also process, organizational and cultural innovation. Bureaucratic turf wars – information technologists versus business practitioners, those who want to maintain control of information and those who think they should have access to it – are likely to continue for some time. These human elements are possibly the greatest unknowns that will continue to challenge COIs.

6. Acknowledgements

The views, opinions, and conclusions expressed in this paper are those of the authors and should not be construed as an official position of the United States Department of Defense. All information presented here is unclassified, technically accurate, contains no critical military technology and is not subject to export controls.

7. References

[1] DoD CIO Memorandum, *Interoperability and Data Management*, December 2001.

[2] DoD CIO, *DoD Net-Centric Data Strategy*, March 2003.

[3] DoD Directive 8320.2, *Data Sharing in a Net-Centric DoD*, December 2004.

[4] Deputy Assistant Secretary of Defense (Deputy CIO), *DoD Discovery Metadata Specification*, July 2005.

[5] DoD *Metadata Registry and Clearinghouse (MDR)*, http://metadata.dod.mil.

[6] Assistant Secretary of Defense (Networks and Information Integration) / DoD CIO, *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, July 2006.